

SSD技术社区SSDFans核心成员撰写，产业界和学术界10余位专家高度评价并推荐
从产品、技术和应用三个维度系统、全面讲解SSD的产品形态、整体架构、工作原理，
以及各个功能模块



深入浅出SSD

固态存储核心技术、原理与实战

SSDFans◎著



机械工业出版社
China Machine Press

深入浅出SSD：固态存储核心技术、原理与实战

SSDFans 著

ISBN: 978-7-111-59979-1

本书纸版由机械工业出版社于2018年出版，电子版由华章分社（北京华章图文信息有限公司，北京奥维博世图书发行有限公司）全球范围内制作与发行。

版权所有，侵权必究

客服热线：+ 86-10-68995265

客服信箱：service@bbbvip.com

官方网址：www.hzmedia.com.cn

新浪微博 @华章数媒

微信公众号 华章电子书（微信号：hzebook）

目录

赞誉

推荐序一

推荐序二

前言

第1章 SSD综述

1.1 引子

1.2 SSD vs HDD

1.3 固态存储及SSD技术发展史

1.4 SSD基本工作原理

1.5 SSD产品核心参数

1.5.1 基本信息剖析

1.5.2 性能剖析

1.5.3 寿命剖析

1.5.4 数据可靠性剖析

1.5.5 功耗和其他剖析

1.5.6 SSD系统兼容性

1.6 接口形态

1.6.1 2.5寸

1.6.2 M.2

1.6.3 BGA SSD

1.6.4 SDP

1.6.5 U.2

1.7 固态存储市场

1.7.1 SSD正在取代HDD

1.7.2 SSD、HDD应用场合

1.7.3 SSD市场情况

第2章 SSD主控和全闪存阵列

2.1 SSD系统架构

2.1.1 前端

2.1.2 主控CPU

2.1.3 后端

2.2 SSD主控厂商

2.2.1 Marvell主控

2.2.2 三星主控

2.2.3 国产主控，谁主沉浮

2.3 案例：硅格（SiliconGo）SG9081主控

2.4 案例：企业级和消费级主控需求的归一化设计

2.5 案例：DERA（得瑞领新）NVMe控制器TAI和NVMe SSD产品

2.6 全闪存阵列AFA

2.6.1 整体解剖

2.6.2 硬件架构

2.6.3 软件架构

2.6.4 工作流程

2.6.5 应用场景

2.7 带计算功能的固态硬盘

第3章 SSD存储介质：闪存

3.1 闪存物理结构

3.1.1 闪存器件原理

3.1.2 SLC、MLC和TLC

3.1.3 闪存芯片架构

3.1.4 读、写、擦原理

3.1.5 三维闪存

3.1.6 Charge Trap型闪存

3.1.7 3D XPoint

3.2 闪存实战指南

3.2.1 异步时序

3.2.2 同步时序

3.2.3 闪存命令集

3.2.4 闪存寻址

3.2.5 读、写、擦时序

3.2.6 ONFI与Toggle协议之争

3.3 闪存特性

3.3.1 闪存存在的问题

3.3.2 寿命

3.3.3 闪存测试

3.3.4 MLC使用特性

3.3.5 读干扰

3.3.6 闪存数据保存期

3.4 闪存数据完整性

3.4.1 读错误来源

3.4.2 重读

- 3.4.3 ECC纠错码
 - 3.4.4 RAID
 - 3.4.5 数据随机化
- 第4章 SSD核心技术: FTL
 - 4.1 FTL综述
 - 4.2 映射管理
 - 4.2.1 映射种类
 - 4.2.2 映射基本原理
 - 4.2.3 HMB
 - 4.2.4 映射表刷新
 - 4.3 垃圾回收
 - 4.3.1 垃圾回收原理
 - 4.3.2 写放大
 - 4.3.3 垃圾回收实现
 - 4.3.4 垃圾回收时机
 - 4.4 Trim
 - 4.5 磨损平衡
 - 4.6 掉电恢复
 - 4.7 坏块管理
 - 4.7.1 坏块来源
 - 4.7.2 坏块鉴别
 - 4.7.3 坏块管理策略
 - 4.8 SLC cache
 - 4.9 RD&DR
 - 4.10 Host Based FTL
 - 4.10.1 Device Based FTL的不足
 - 4.10.2 Host Based FTL架构
 - 4.10.3 百度的软件定义闪存
- 第5章 PCIe介绍
 - 5.1 从PCIe的速度说起
 - 5.2 PCIe拓扑结构
 - 5.3 PCIe分层结构
 - 5.4 PCIe TLP类型
 - 5.5 PCIe TLP结构
 - 5.6 PCIe配置和地址空间
 - 5.7 TLP的路由
 - 5.8 数据链路层

- 5.9 物理层
- 5.10 PCIe Reset
- 5.11 PCIe Max Payload Size和Max Read Request Size
- 5.12 PCIe SSD热插拔
- 5.13 SSD PCIe链路性能损耗分析
- 第6章 NVMe介绍
 - 6.1 AHCI到NVMe
 - 6.2 NVMe综述
 - 6.3 吉祥三宝: SQ、CQ和DB
 - 6.4 寻址双雄: PRP和SGL
 - 6.5 Trace分析
 - 6.6 端到端数据保护
 - 6.7 Namespace
 - 6.8 NVMe over Fabrics
- 第7章 SSD测试
 - 7.1 主流SSD测试软件介绍
 - 7.1.1 SSD性能测试第一神器——FIO
 - 7.1.2 AS SSD Benchmark
 - 7.1.3 ATTO Disk Benchmark
 - 7.1.4 CrystalDiskMark
 - 7.1.5 PCMark Vantage
 - 7.1.6 IOMeter
 - 7.2 验证与确认
 - 7.3 测试仪器
 - 7.3.1 Emulator
 - 7.3.2 协议分析仪
 - 7.3.3 Jammer
 - 7.4 回归测试
 - 7.5 DevSlp测试
 - 7.6 PCIe InterOp
 - 7.7 WA测试
 - 7.8 耐久度测试
 - 7.9 认证Certification
 - 7.10 SSD Performance测试
- 第8章 SSD电源管理
 - 8.1 SATA省电模式Partial和Slumber
 - 8.2 SATA超级省电模式DevSlp

- 8.3 SATA终极省电模式RTD3
- 8.4 PCIe省电模式ASPM
- 8.5 PCIe其他省电模式
- 8.6 NVMe动态电源管理
- 8.7 Power Domain
- 第9章 ECC原理
 - 9.1 信号和噪声
 - 9.2 通信系统模型
 - 9.3 纠错编码的基本思想
 - 9.3.1 编码距离
 - 9.3.2 线性纠错码的基石——奇偶校验 (Parity-Check)
 - 9.3.3 校验矩阵 H 和生成矩阵 G
 - 9.4 LDPC码原理简介
 - 9.4.1 LDPC是什么
 - 9.4.2 Tanner图
 - 9.5 LDPC解码
 - 9.5.1 Bit-flipping算法
 - 9.5.2 和积信息传播算法
 - 9.6 LDPC编码
 - 9.7 LDPC在SSD中的应用
 - 9.7.1 NAND会出错
 - 9.7.2 NAND纠错模型
 - 9.7.3 LDPC纠错流程

赞誉

(排名不分先后)

随着闪存技术的发展和智能终端对数据交互性能的要求日趋提高，SSD被越来越多地应用于各种场景中。本书围绕SSD的产品、技术、应用等角度展开阐述，既严谨又全面，给SSD的从业人员和爱好者们提供了一个完整的视图。

——陈强 硅格半导体市场总监

本人从2008年起加入固态硬盘行业。相信大多数从业者跟我的感觉一样：希望能够系统而深入地学习固态硬盘技术，但国内却很难找到一本专业书籍。本书对固态硬盘工作原理、接口形态、市场应用等基础知识，以及控制器底层的各种算法，都进行了详尽介绍。无论是对于固态硬盘行业的从业者、技术开发者、市场人员，还是对于投资人、终端用户，本书都是不可或缺的学习和参考经典。

——楚一兵 深圳市瑞耐斯技术有限公司CEO

固态存储无疑已成为主流，从移动装置到云，都已全面应用。本书从固态硬盘的发展史到技术应用，都进行了专业剖析和详细说明，让读者可以一次性透彻了解固态存储的来龙去脉，是值得一读及收藏的专业书籍。

——段喜亭 慧荣科技市场营销暨OEM事业资深副总

存储领域的中文技术书籍一直比较匮乏，关于SSD固态存储的书籍更是如此。听说这本书汇集了SSDFans五位运营者一年的努力，深感不易。再看目录也是大而全，从底层到应用，从NAND介质到闪存系统，从知识普及到深入的技术细节，全都有深入剖析。无论是SSD相关从业者，还是技术爱好者，这部全面而系统的著作都值得大家学习、参考。

——黄亮 《企业存储技术》微信公众号作者

作为硬件领域最重要的革命之一——闪存革命正在深刻地改变着IT的基础架构，并改变着人们获取信息的方式。理解闪存区别于磁性介质的特点和SSD不同于HDD的“怪脾气”，对于高效存储架构设计极为关键。这本书带我们近距离观察SSD在最近十多年的发展演进，并结合闪存的特点把通信、计算机等技术贯穿起来，实现一个接近理想的、高效的和可靠的存储架构。

——路向峰 忆恒创源CTO

推荐序一

信息存储记录历史、传承文明，是人类社会延续和发展不可或缺的重要手段。一个时代有多种存储介质，但总有一种存储介质是主流介质。古埃及人用的莎草纸、早期欧洲人用的羊皮纸、中国人用的竹简以及后来的纸张，都曾作为主流介质被广泛使用。进入数字时代，以硬盘为核心的磁记录介质一直是非易失性存储的主流介质。然而，由于闪存（Flash Memory）技术的迅猛发展，这种局面即将发生重大转变。闪存介质在各类存储卡、固态硬盘和全闪存阵列中大量应用，不论在终端还是在云端，闪存已无处不在。闪存介质中存储的人类社会信息总量将在不久的将来超过磁记录介质，成为数字时代新的主流存储介质。

固态硬盘（Solid State Disk, SSD）是以闪存介质为主的一种极为重要的存储产品，它广泛应用于移动终端、笔记本电脑、台式机、服务器和数据中心等场合，需求量极大。与传统的机械硬盘相比，固态硬盘的性能优势特别突出。由于取消了机械部件，旋转和寻道的延迟完全消除，固态硬盘在读写速度上远优于机械硬盘，特别是在大吞吐率的随机读写性能上有了几个数量级的提高，在性能要求高的应用场合已成为首选。与机械硬盘相比，固态硬盘的容量和价格曾是其成为主流的障碍。但随着闪存芯片容量的迅速增加和成本的快速下降，固态硬盘的最大容量已超过机械硬盘，单位容量价格也日益趋近高性能机械硬盘的价格，并将在未来的几年之中与之持平，之后将逐步取代大容量机械硬盘。

对固态硬盘这样一种量大面广的重要存储设备，无论是其设计者、生产者还是应用者，都迫切希望对其工作原理和关键技术有一个全面的了解。然而，目前关于固态硬盘的各种知识和资料散落于各类学术论文和网上的技术介绍，市面上系统介绍固态硬盘技术的书籍并不多见。本书的出版恰逢其时，满足了广大读者的需求，是一本全面介绍固态硬盘技术的书籍。

固态硬盘一般采用NAND闪存芯片作为基本组件，对闪存芯片特性的透彻了解是理解固态硬盘工作原理的基础。NAND闪存用电荷存储信息，其重要特点是先擦后写，擦写寿命有限。随着密度提高，引起了单元电荷数的减少及绝缘层变薄，从而使得NAND闪存的原始误

码率不断提高，可擦写次数也越来越差，最新的大容量芯片擦写寿命不到1千次。用这样一种高误码率、短寿命的芯片来构成长寿命、高性能、高可靠的固态硬盘，需要发展一系列系统层面的技术，如地址映射、磨损均衡、垃圾回收、坏块管理等，还需要发展新的纠错编码理论、算法和实现技术来保证数据的正确性和可靠性。为了能与主机进行高性能连接与通信，需要发展与固态介质相适应的高速接口和通信协议。上述系统层面的技术不仅需要特别设计的硬件控制器来实现，还需要底层固件的支持。固态硬盘品质的优劣，不仅反映在初期使用的性能上，还反映在大负载长期使用后性能和可靠性的保持能力上，故需要发展与固态硬盘相适应的评测技术。上述内容都是因固态硬盘的出现而发展出来的新技术和新知识，本书以一种深入浅出的风格系统地阐述了这些内容。

值得特别指出的是，本书作者不仅是在第一线从事固态硬盘设计、有着深厚专业知识的资深工程师，还是一群热衷于普及固态硬盘知识的写作高手。他们创立了SSDFans微信群和微信公众号，发表了大量关于固态硬盘技术和市场的文章，尤其在技术内容的阐述上形成了深入浅出、通俗幽默的写作风格，读来使人兴趣盎然。我就经常进入这个微信群阅读那些十分有趣的短文，获得了不少新的技术知识和市场信息。本书延续了SSDFans微信群的写作风格，相信读者在阅读时一定会体验到其中的乐趣。

我国在磁记录介质时代错失了大力发展硬盘产业的机会，从而导致使用数量十分惊人的硬盘全部依赖进口。除了花费巨量外汇之外，信息安全也存在着问题。我国已意识到信息存储产业的极端重要性，大力发展闪存产业已成为国家意志。我国已投入巨资建立3D闪存芯片制造基地，有望解决基础器件的问题。为了使我国成为闪存时代国际舞台上的主角，建立包括芯片颗粒、控制器、固态硬盘和盘阵等环节的全产业链十分必要。固态硬盘不仅是量大面广的产品，也是连接闪存上下游产业最重要的一环。相信本书的出版能推动固态硬盘技术知识的普及，促进我国固态硬盘产业发展和应用，并在人才培养方面发挥积极作用。

闪存成为主流存储介质的时代来临，国际舞台将精彩纷呈，中国一定不能缺席。

谢长生 教授

华中科技大学武汉光电国家研究中心

信息存储系统教育部重点实验室

推荐序二

作为《大话存储（终极版）》以及《大话存储（后传）》的作者，我有幸经历了国内存储行业发展的启蒙和鼎盛时代。在2005年到2013年这8年间，存储市场基本就是SAN的市场，谈存储必暗指SAN。但是从2014年往后，存储行业突然发生巨大变化，分布式系统和固态存储介质开始呈爆发式增长。今天，谈存储如果不谈一谈配以固态硬盘的分布式系统，就仿佛是上个时代的人了。

分布式系统的发展有三个技术条件：高速网络、大容量硬盘、固态介质。这三者彻底解放了分布式系统的生产力。通俗一点说也就是：网络快了、盘容量大了、盘速度快了。高速网络是分布式系统赖以生存的根本，分布式存储系统早在20世纪中后期就已经形成了理论基础，但是一直到近几年，网络的时延和带宽才足以支撑分布式系统架构。为了降低成本，业界兴起所谓软件定义，也就是利用廉价白牌机或者标准的机架服务器，加上分布式存储软件管理层，搭建出软件定义分布式存储系统，与传统的SAN存储系统瓜分市场。而分布式系统的大行其道，极大地促进了固态存储的需求量，因为出于成本考量，分布式系统中每个节点往往不会连接多级JBOD从而靠大量的硬盘形成高并发性能，而是只靠每个服务器自带的少量盘位，加上固态盘来抵消跨网络通信带来的时延增加，形成让传统机械盘系统望尘莫及的IOPS和时延性能。

可以说，固态存储对系统架构和存储市场都有着颠覆性的影响。构建在大量机械硬盘基础之上的传统SAN存储架构不得不为固态存储重新定制，而固态存储让整个存储系统架构变得更加简单，这样SAN存储的门槛更低了，从而失去了核心竞争力。目前采用传统SAN存储架构的存储系统相比新兴存储系统，唯一一个不可撼动的优势就是其高可靠性，体现在两方面：一是硬件部件双冗余设计；二是在硬盘、HBA卡可靠性方面长期积累的经验。

固态存储近年来在国内的发展势头迅猛，造就了众多本土的、自主研发的、与闪存相关的企业，其中有些为SSD整盘提供商，有些为自主研发SSD主控的企业，有些为盘和主控兼有的企业。长期以来，机械硬盘的核心技术被少数几家企业掌控，门槛极高。而固态存储的入门门槛极大降低，在研发NAND主控方面，相比于机械硬盘，无论

是在技术储备、技术实现上，还是在人员、物料成本上，都变得可以接受。然而，这并不意味着NAND闪存及其控制器、固件等一整套系统可以被轻易驾驭。闪存技术领域包含很多的复杂概念及复杂算法，比如SLC/MLC/TLC/QLC、3D NAND、快慢页、上下页、局部/全局磨损均衡、擦1写0、垃圾回收、Device/Host Based FTL、元数据保护机制、页面映射、NVMe、PCIE/SATA/SAS、SPDK/DPDK、RDMA、NVMe Over Fabric、LDPC/BCH等，这些概念相比传统存储系统更加接近底层和也更加精细，需要更高的学习成本。

业界迫切需要一本全面阐述、梳理固态存储底层技术的图书。本书的面世，可谓是雪中送炭，其及时满足了广大固态存储行业从业者学习了解固态存储相关知识的需求。

SSDFans团队由知名闪存控制器厂商的工程师组成，维护着SSDFans微信公众号，以较高频率发布与各类固态存储相关的技术或市场类文章。我也是SSDFans的粉丝之一，从SSDFans的文章中学到不少知识。写书不易，写出一本符合人脑认知原生态思维路径的书更不易。作为全面、系统、深度介绍固态存储技术、产品的书籍，本书语言通俗易懂，脉络清晰。本书不仅可以作为固态存储行业的入门书，也可以作为广大固态存储行业从业者常备的参考书。对于已经非常资深的固态存储行业人员来说，也是开卷有益，因为通过本书他们可查漏补缺，重新梳理思路。

我强烈推荐本书！

冬瓜哥

前言

为什么要写这本书

这是一个真正的数据大爆炸时代，看得见，摸得着。

我们每天都在生产数据：发朋友圈、发微博、上传图片和视频到社交网站、备份数据到网盘等。我们的这些数据，不是存储在虚无缥缈的云端，而是存储在云服务器上。云服务器的核心就是存储介质。无论是云端存储，还是本地存储，有数据的地方就有存储介质。

传统数据存储介质有磁带、光盘等，但更多的是硬盘（HDD）。随着数据呈爆炸式增长，对数据存储介质在速度上、容量上有更高的要求。时势造英雄，固态硬盘（Solid State Disk, SSD）横空出世。SSD使用电子芯片存储数据，没有HDD的机械式部件，因此在速度、时延、功耗、抗震等方面，与HDD相比有碾压式优势。无论是个人存储，还是企业存储，都在逐渐用SSD取代HDD。大数据时代，SSD必将是主角。

HDD时代我们错过了；SSD时代，我们迎来了弯道超车的好机会。国内很多企业都希望抓住这个机遇，所以他们研发、制造SSD，并且取得了不错的成绩，已经有了能自主研发SSD及SSD控制器的公司。国家层面也在大力研发半导体。长江存储的成立昭示了国家对固态存储这块的态度和决心。

国内SSD领域的从业人员，以及日常使用SSD的人越来越多，但是市面上专门介绍SSD技术的中文书籍少之又少。作为国内领先的SSD技术社区——SSDFans有责任、有义务，也有动力推出一本中文版SSD技术书籍。

我们几位作者，都工作在SSD的最前线，是工程师出身，虽文笔一般但是热情十足，愿意分享对技术的理解。希望这块砖头能够帮助您敲开SSD的大门，如果能够解决您的一些实际问题，或者引发您的一些思考，我们更是不胜荣幸。

最后，欢迎您通过网站（<http://www.ssdfans.com>）、微信公众号（SSDFans）来进一步了解我们，与我们做进一步的交流。

读者对象

·计算机、电子相关专业的在校本科生，存储方向的研究生：通过阅读本书，能够更好地将所学的理论 with 业界实践结合，对相关知识有更加深刻的理解，为未来加入企业打好坚实的基础。

·SSD研发企业的员工：通过阅读本书，可以全面学习与SSD相关的硬件、协议、固件以及测试等各方面的基础知识，提升整体认知，具备完整、系统的理论知识。

·企业IT运维人员：通过阅读本书，可以充分了解SSD的优劣之处及其适用的工作场景，为公司的IT部署过程提供技术支持，实现整体运营成本的最优配置。

·广大的DIY、游戏爱好者：通过阅读本书，可以学会如何选择最适合自己的SSD，以合理投入获得更好的娱乐体验。

·对SSD产业感兴趣的投资人：通过阅读本书，可以全面了解SSD产业的现状，掌握基本的技术术语，以便更好地与企业沟通。

·其他对SSD知识感兴趣的人。

本书特色

本书的作者团队都在业内知名公司任职，具备丰富的理论和实践知识。同时，日常维护公众号期间，跟读者的频繁互动也保证了知识的更新速度。

在撰写本书的过程中，作者们能够对技术原理做深入浅出的阐述，并结合自身工作经验给出意见。

本书主要内容

本书的内容几乎覆盖了SSD各个模块，既可以作为一本入门书籍进行通读，也可以在需要的时候作为工具书进行查阅。

本书内容涵盖：**SSD基础知识**、**SSD各模块介绍**及**SSD测试相关内容**。

SSD基础知识包括：**SSD与HDD的比较**、**SSD的发展历史**、**产品形态**、**整体架构**和**基本工作原理**。

模块介绍包括：

- FTL闪存转换层**：作为SSD固件的核心部分，FTL实现了例如映射管理、磨损均衡、垃圾回收、坏块管理等诸多功能，本书将一一介绍。

- NAND Flash**：NAND Flash作为SSD的存储介质，具有很多与传统磁介质不同的特性，本书将从器件原理、实战指南、闪存特性及数据完整性等方面展开。

- NVMe存储协议**：作为专门为SSD开发的软件存储协议，NVMe正在迅速占领SSD市场。本书将从其优势、基础架构、寻址方式、数据安全等方面展开。为了让读者对NVMe命令处理有更加直观的认识，本书结合实际的PCIe trace进行阐述。同时，本书也介绍了NVMe Over Fabric的相关知识，让读者能够对未来网络与存储的发展趋势有所了解。

- PCIe协议**：PCIe作为目前主流的SSD前端总线，与之前的SATA接口相比有着极大的性能优势。本书将从PCIe总线拓扑结构、分层结构、TLP类型与路由、配置和地址空间等方面进行介绍。

- 电源管理**：本书详述了SSD前端总线（包括SATA和PCIe）的各种节能模式、NVMe协议的电源管理方案及在SSD里常用的整体电源管理架构——Power Domain。

- ECC**：本书介绍了ECC的基本概念，重点介绍了LDPC的解码和编码原理，以及在NAND上的应用。

SSD测试的内容包括：本书详述了常用的测试软件、测试流程、仪器设备、业界认证及专业的测试标准等。

勘误和支持

由于作者的水平有限，再加上时间仓促，书中难免会出现一些错误或者不准确的地方，恳请读者批评指正。您可通过我们的网站（<http://www.ssdfans.com>）、微信公众号（或微博）SSDFans、阿呆的微信号（nanoarchplus）或阿呆的邮箱（adam@ssdfas.com）随时与我们进行交流。

致谢

借此机会特别感谢一直以来支持SSDFans的各位朋友（排名不分先后）——冬瓜哥、唐杰、路向峰、廖莎、兵哥、邵总、古猫先生、袁戎、顾沧海、山哥（Brown）等。

感谢机械工业出版社华章公司的编辑杨福川和孙海亮，在这一年多的时间中他们始终支持我们这几个门外汉，他们的鼓励和帮助引导我们顺利完成全部书稿。

谨以此书献给亲爱的家人，以及众多支持SSDFans的朋友们！

第1章 SSD综述

SSD (Solid State Drive)，即固态硬盘，是一种以半导体闪存 (NAND Flash) 作为介质的存储设备。和传统机械硬盘 (Hard Disk Drive, HDD) 不同，SSD以半导体存储数据，用纯电子电路实现，没有任何机械设备，这就决定了它在性能、功耗、可靠性等方面和HDD有很大不同。其实SSD的概念很早就有，但真正成为主流存储应用还是最近10年的事情。在2008年初，那时候只有很少的几家公司研发SSD，如今 (2018年)，已有上百家大小的公司参与其中。无论是在消费级还是企业级市场，SSD已经动了两家HDD巨无霸公司——西数 (WD) 和希捷 (Seagate) 的根基，正在取代HDD成为主流的存储设备。

在SSD大行其道的今天，从事存储行业的人如果不知道SSD，犹如“平生不见陈近南，就称英雄也枉然”。本章将带领大家初识“陈近南”。

1.1 引子

先从开机速度说起。

过去，电脑启动一般需要几十秒甚至一分钟以上。开机，出去倒茶，回来，电脑还在打转转。如今，使用了SSD后，开机只要几秒钟。开机，正起身准备去倒茶，开机助手就已经提示你：本次开机8秒钟，击败全国99%的用户。算了，茶还是不倒了。SSD开机时间统计如图1-1所示。

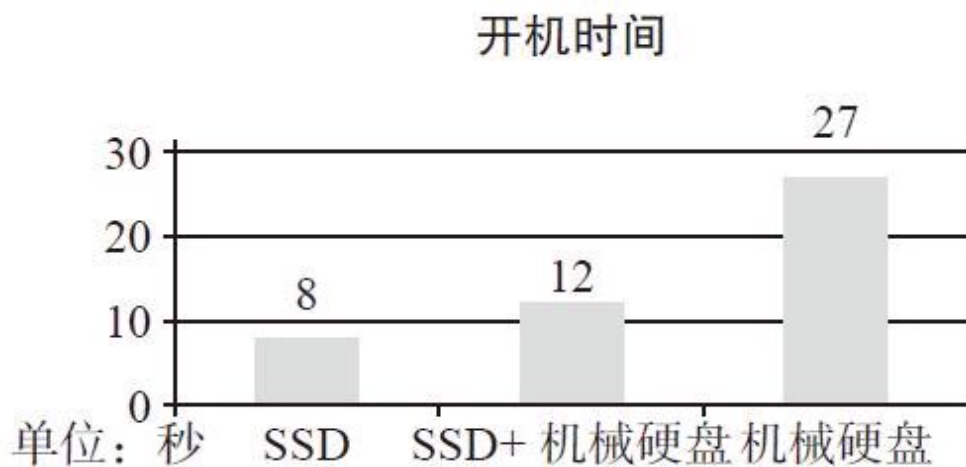


图1-1 SSD开机时间统计

速度快，是用户在使用SSD过程中最为直观的感受。那是什么成就了SSD的神速呢？除了速度快，相比HDD，SSD还有什么优点呢？这就得从SSD的原理说起了。

SSD是一种以半导体为主要存储介质、外形和数据传输接口与传统的HDD相同的存储产品。目前主流SSD使用一种叫闪存的存储介质，未来随着存储半导体芯片技术的发展，它也可以使用更快、更可靠、更省电的新介质，例如3D XPoint、MRAM等。由于当前业界主要使用的还是闪存，所以本书讨论还是以闪存为主。

外观上，加上铝盒的2.5寸的SSD，和2.5寸HDD外观基本相同。除了有传统HDD的2.5寸和3.5寸的外观外，SSD还可以有更小的封装和尺寸，图1-2所示为M.2接口的SSD。（关于SSD的接口形态，后续有详细的介绍。）

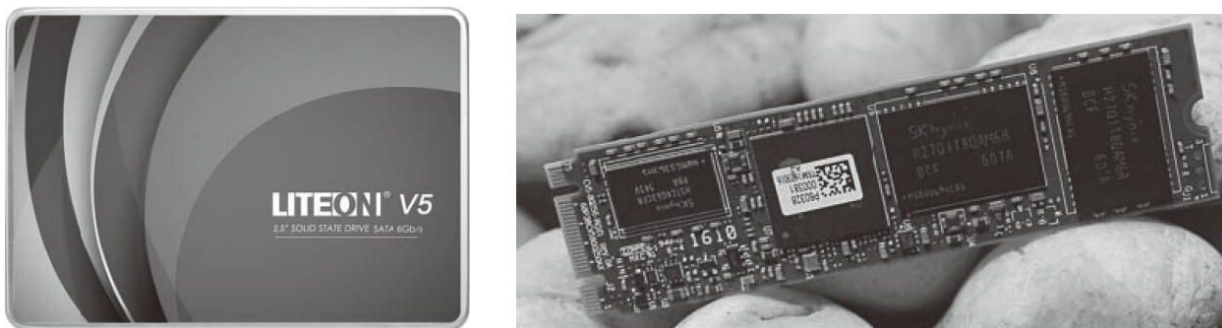


图1-2 SSD外观（左：2.5寸盘；右：M.2SSD）

SSD是用固态电子存储芯片阵列制成的硬盘，主要部件为控制器和存储芯片，内部构造十分简单。详细来看，SSD硬件包括几大组成部分：主控、闪存、缓存芯片DRAM（可选，有些SSD上可能只有SRAM，并没有配置DRAM）、PCB（电源芯片、电阻、电容等）、接口（SATA、SAS、PCIe等），其主体就是一块PCB，如图1-3所示。软件角度，SSD内部运行固件（Firmware，FW）负责调度数据从接口端到介质端的读写，还包括嵌入核心的闪存介质寿命和可靠性管理调度算法，以及其他一些SSD内部算法。SSD控制器、闪存和固件是SSD的三大技术核心，后面章节会依次深度介绍。

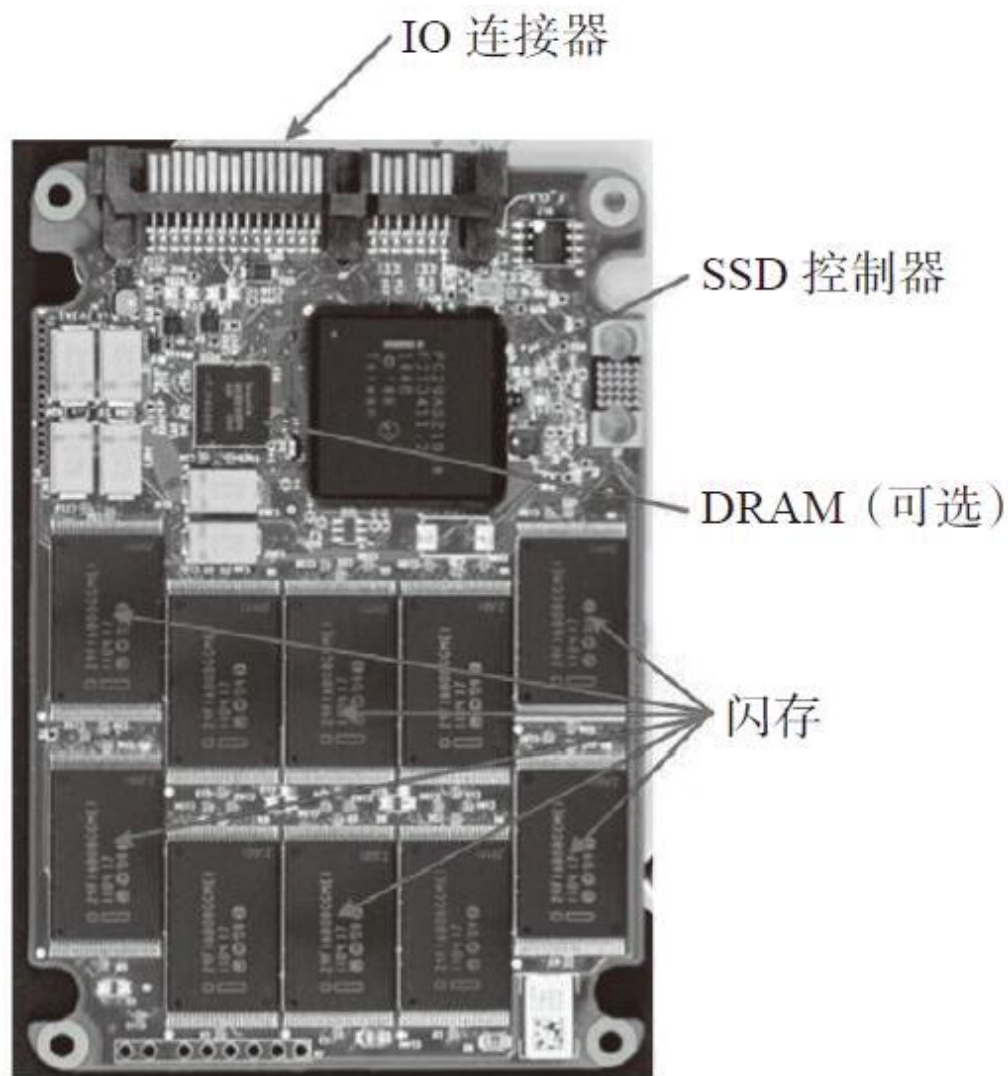


图1-3 SSD结构

前面讲了当前SSD存储介质主要是闪存，故首先讲一下什么是存储介质。

存储介质按物理材料的不同可分为三大类：光学存储介质、半导体存储介质和磁性存储介质。光学存储介质，就是大家之前都使用过的DVD、CD等光盘介质，靠光驱等主机读取或写入。在SSD出现之前，个人和企业的数据存储还是HDD的天下，HDD是以磁性存储介质来存储数据的；SSD出现以后，采取的是半导体芯片作为存储介质。现在及未来技术变革最快和主要方向还是半导体存储，从图1-4可以看出，半导体存储介质五花八门，目前可以看得出的主要方向还是闪存、3D XPoint、MRAM、RRAM等。

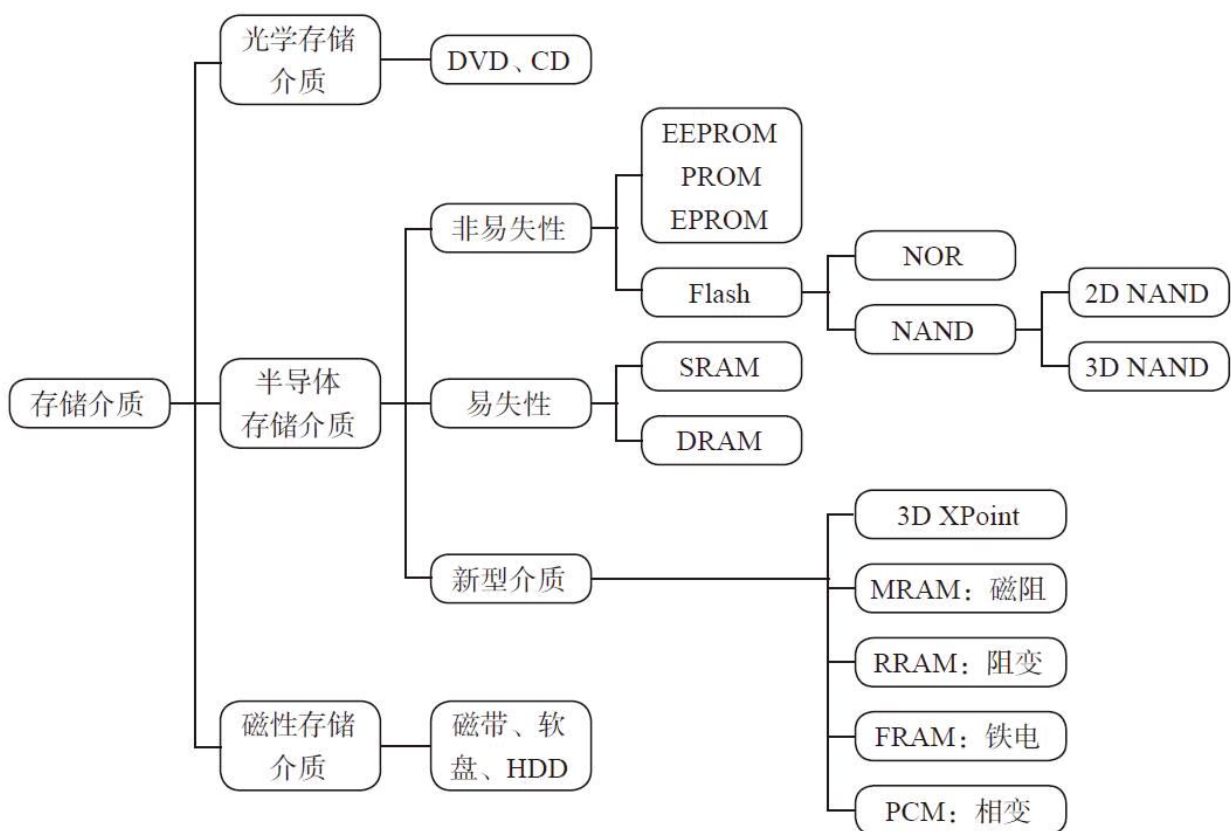


图1-4 存储介质分类

当前闪存生产供应商主要有Micron（美光）、Samsung（三星）、SK Hynix（现代海力士）、Toshiba（东芝）、WD&Sandisk（西数和闪迪），这几家基本上垄断了闪存市场，当然未来会有新的加入者，给用户以更多的选择。

1.2 SSD vs HDD

传统的HDD是“马达+磁头+磁盘”的机械结构，SSD则变成了“闪存介质+主控”的半导体存储芯片结构，两者有完全不同的数据存储介质和读写方式。对比如表1-1所示。

再看一下SSD和HDD物理结构的不同，如图1-5所示。

表1-1 HDD vs SSD结构对比

	方式	数据存储介质	读取写入
HDD	机械	磁盘（磁性介质）	磁头 + 马达（寻址）
SSD	电子	闪存	SSD 控制器

从技术参数上来看，SSD与HDD相比具有如下优点。

1.性能好

毫无疑问，SSD在速度上可以秒杀HDD，无论在用户感观体验上，还是测试数据上。

表1-2所示是某两款SSD和HDD的对比，由表可以看到的是，读写速度有从几倍到几百倍的差异，随机读写性能（速度和时延）差异最为明显。

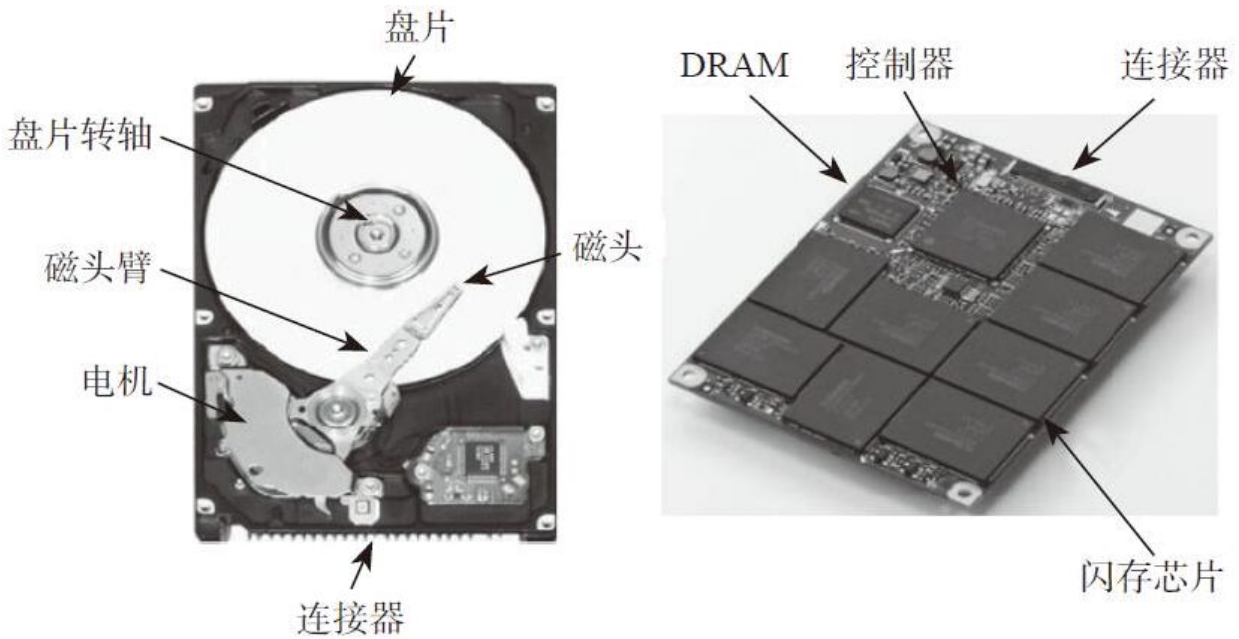


图1-5 SSD vs HDD结构
表1-2 HDD与SSD性能对比

	SATA SSD (500GB)	SATA HDD (500GB 7 200rpm)	区别
介质	闪存	磁盘	
连续读 / 写 (MB/s)	540/330	160/60	× 3/ × 6
随机读 / 写 (IOPS)	98 000/70 000	450/400	× 217/175
数据访问时间 (ms)	0.1	10 ~ 12	× 100 ~ 120
性能得分 (PCMark)	78 700	5 600	× 14

性能测试工具包括连续读写吞吐量 (Throughput) 工具和随机读写 IOPS 工具两种，包括但不限于 IoMeter、FIO 等测试工具。也有用户体验的性能测试工具——PCMark Vantage，它以应用运行和加载时间作为考察对象。性能测试项一般都是影响用户体验的项。影响用户体验的项涉及系统启动时间、文件加载、文件编辑等。从图1-6所示的对比可以看出，HDD的得分在SSD面前显得太渺小，像碰见了一个性能怪兽，被完爆。

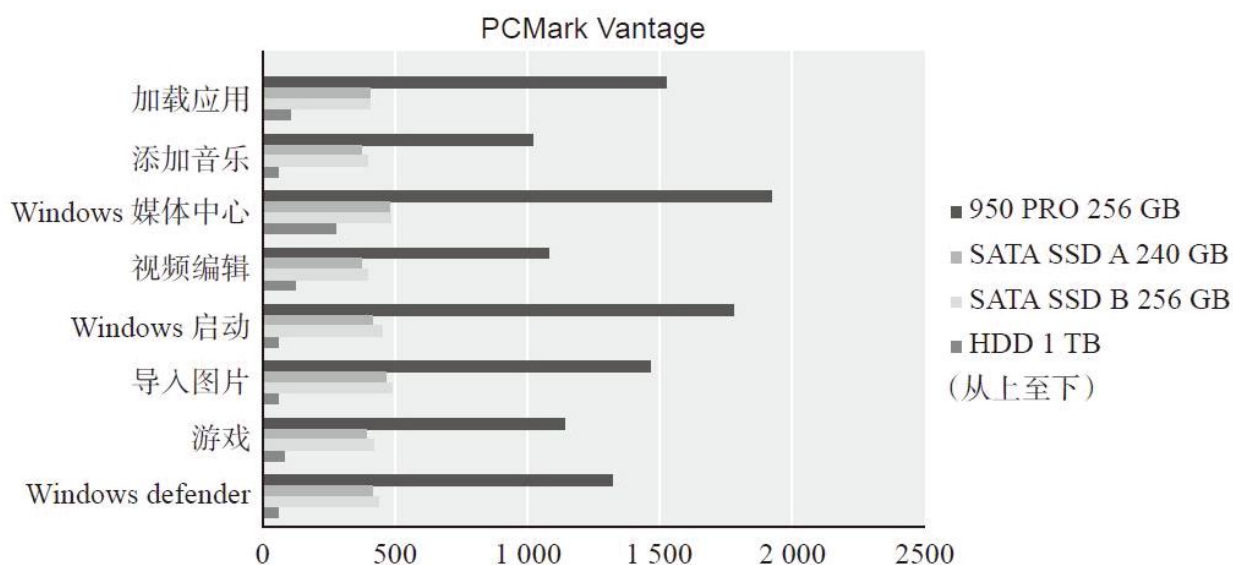


图1-6 SSD vs HDD性能得分

2.功耗低

工作功耗HDD为6~8W，SATA SSD为5W，待机功耗SSD可降低到毫瓦（mW）级别。

关于功耗，业界定义有几类：峰值功耗（Peak Power）、读写功耗（Active Power）、空闲功耗（Idle Power）、省电功耗（启动SSD内部休眠，尽可能多地关掉不工作的硬件模块，专业上定义为Standby/Sleep Power和DevSleep Power，本书后面有专门章节介绍）。特别是DevSleep Power，功耗可降到10mW以下，功耗极低，可应用于能耗要求苛刻的应用场景，如消费级笔记本休眠状态，此种场景下SSD省电是非常重要的。HDD与SSD的功耗对比如表1-3所示。

表1-3 HDD与SSD功耗对比

	峰值功耗（W）	读写功耗（W）	睡眠功耗（mW）	深度睡眠功耗（mW）
HDD	8	6	500	不支持
SATA SSD	6	5	100	5
PCIe SSD	25	15	200	10

从SSD功耗分解来看，读写功耗主要消耗在闪存上。数据读取和写入并发在后端的闪存，闪存的单位读写功耗是决定性的，如16KB闪存页（Page）的读写功耗决定了主机端满负荷下SSD的平均读写功耗。

其次影响读写功耗的是主控功耗，其约占功耗的20%，而ASIC主控CPU的频率和个数、后端通道的个数、数据ECC的编码器/解码器的个数和设计等因素影响了主控整体的功耗。

科学地比较功耗的方法应该是Power/IOPS，也就是比较单位IOPS性能上的功耗输出，该值越低越好。由于SSD极高的性能，相对于HDD而言，相当于单位功耗产生出了百倍的性能，所以SSD被称为高性能、低功耗的节能产品，符合数据中心（Data Center）的使用定位。

3.抗震防摔

SSD内部不存在任何机械部件，相比HDD更加抗震。

HDD是机械式结构，磁头和磁片之间发生跌落时接触碰撞会产生物理损坏，无法复原。SSD是电子和PCB结构，PCB加半导体芯片，跌落时不存在机械损伤问题，因此更加抗震和可靠。

另外SSD对环境的要求没有HDD那么苛刻，更适合作为便携式笔记本、平板电脑的存储设备。从可靠性角度来看，物理上的损伤以及带来数据损坏的概率，SSD比HDD更低。

4.无噪声

客观上，由于结构上没有马达的高速运转，SSD是静音的。

5.身形小巧百变

HDD一般只有3.5寸和2.5寸两种形式，SSD除了这两种，还有更小的可以贴放在主板上的M.2形式，甚至可以小到芯片级，例如BGA SSD的大小只有16mm×30mm，甚至可做得更小。

江波龙2017年8月发布了目前世界上最小尺寸的BGA SSD（11.5mm×13mm）——P900系列。

最后再综合对比一下SSD和HDD的具体差异，如表1-4所示。

表1-4 HDD与SSD对比矩阵

比较项	SSD	HDD	比较项	SSD	HDD
容量	√		噪声	√	
性能	√		重量	√	
可靠性	√		抗震	√	
寿命	√		温度	√	
尺寸	√		价格		√
功耗	√				

看来，目前HDD和SSD相比只有价格优势。但随着大容量闪存的出现，SSD的价格也会越来越低，相信不久的将来，HDD的价格优势也会不复存在。

1.3 固态存储及SSD技术发展史

SSD一路走来，从技术层面的发展演进和各个初创公司的涌现，到少数壮大，再到今天汇聚成一股强大的力量，推动SSD的普及应用，可谓不易。回顾SSD的历史，会让我们更深刻地理解这场技术革命对人类生活的改变是多么的艰辛和曲折，真可谓“山重水复疑无路，柳暗花明又一村”。

早在1976年就出现了第一款使用RAM的SSD，1983年Psion公司的计算器使用了闪存存储卡，1991年SanDisk推出了20MB的闪存SSD。经过成千上万科学家、工程师以及各行各业的人40来年的努力，SSD终于改变了我们的生活。下面我们来回顾一下SSD的逆袭之路。

StorageSearch是一家专门讲述各大固态存储公司产品的网站，本节中SSD发展史大部分内容来自于该网站的一篇文章：

<http://www.storagesearch.com/chartingtheriseofssds.html>。

1. 昂贵的RAM SSD时代

我们都知道芯片巨头Intel现在最赚钱的产品是CPU，但是在20世纪70年代，Intel最赚钱的产品是RAM，就是我们电脑内存条里面的芯片。当RAM刚被发明的时候，就有一些脑子灵活的人开始用很多RAM组装成容量很大的硬盘来卖。

据史料记载，1976年，Dataram公司开始出售叫作Bulk Core的SSD，容量是2MB（在当时很大了），使用了8块大电路板，每个板子有18个256KB的RAM（细心的读者肯定在想2MB是怎么算出来的，其实很简单，好好想想吧）。这款SSD是个大块头，具体外观如图1-7所示。

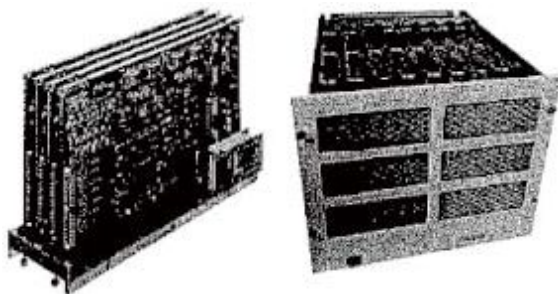


图1-7 Bulk Core SSD

RAM的优点是可以随机寻址，就是每次可以只读写一个字节的数
据，速度很快；缺点也很明显，掉电数据就没了，价格还巨贵。其注
定是土豪的玩具，不能进入寻常百姓家。

在以后的20多年时间里，TMS（Texas Memory Systems）、EMC、
DEC等玩家不断推出各种RAM SSD，在这个小众的市场里自娱自乐。
不过特别强调一下，最主要的玩家是TMS。

2.机械硬盘（HDD）称霸世界

当SSD还在富豪的俱乐部里被把玩的时候，HDD却异军突起，迅
速普及全世界。HDD本来也很昂贵，而且容量小，但是1988年费尔和
格林贝格尔发现了巨磁阻效应，这个革命性的技术使得HDD容量变得
很大，在各大企业的推广下，HDD进入千家万户。他们俩也因此获得
了2007年诺贝尔物理学奖。

2013年全球卖出了5.7亿块HDD，市场为320亿美金。但是，HDD
已经过了最鼎盛的时代。图1-8所示是根据希捷、西部数据和东芝的出
货量做出的全球HDD销量统计，可以看出，从2010年开始，HDD出货
量一直在下滑（2014年有小的反弹）。

单位：亿

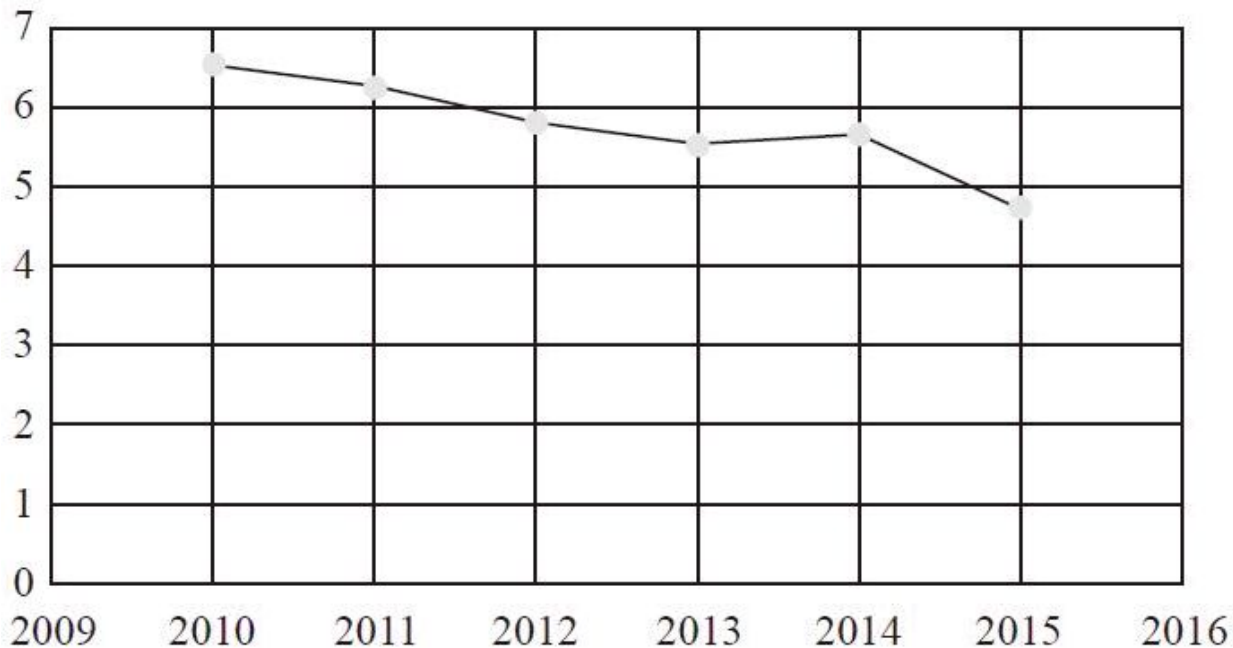


图1-8 全球机械硬盘销量变化

3. 闪存——源于华人科学家的发明

1967年，贝尔实验室的韩裔科学家姜大元和华裔科学家施敏一起发明了浮栅晶体管（Floating Gate Transistor），这是现在SSD基础——闪存的技术来源。学过MOS管的同学肯定对图1-9很熟悉，相比MOSFET就多了个Floating Gate，悬浮在中间，所以叫浮栅。它被高阻抗的材料包裹，和上下绝缘，能够保存电荷，而电荷通过量子隧道效应进入浮栅。

施敏：1936年生于南京，毕业于台湾大学，在斯坦福大学获得博士学位，是著名的物理学家，现于台湾的交通大学任教。期待SSD的普及能让他获得诺贝尔奖。

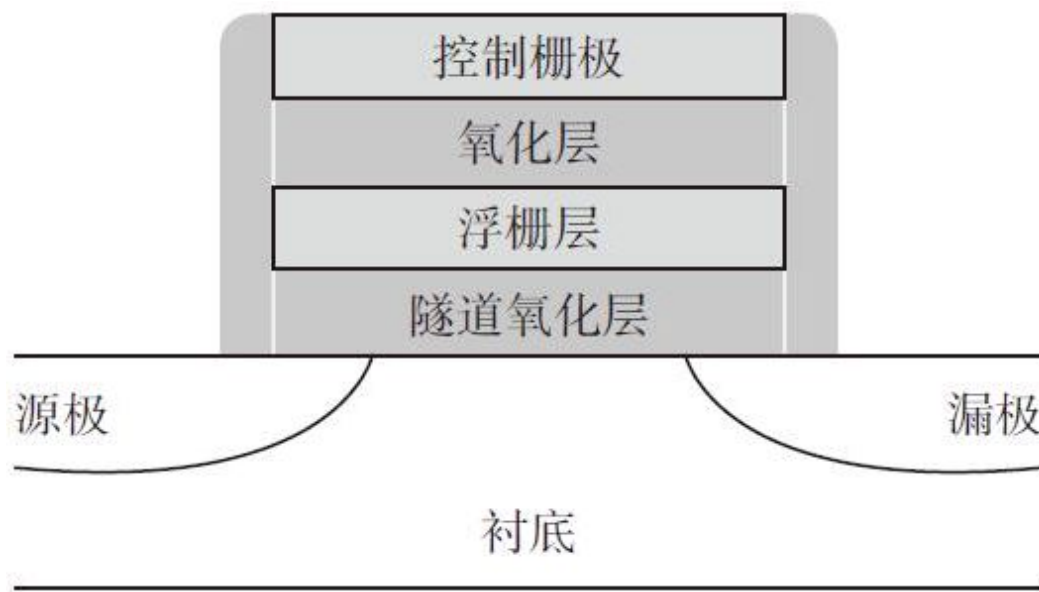


图1-9 浮栅晶体管结构

4. 闪存SSD异军突起

20世纪90年代末，终于有一些厂商开始尝试使用闪存制造SSD，进行艰难的市场探索。1997年，Altec Computer Systeme推出了一款并行SCSI闪存SSD，接着1999年BiTMICRO推出了18GB的闪存SSD，从此，闪存SSD逐渐取代RAM SSD，成为SSD市场的主流。闪存的特点是掉电后数据还在，真的像我们所知的硬盘了。

新技术的应用是如此之快，引起了科技巨头的关注。2002年比尔·盖茨就预见到了SSD的普及，他保守地说，有一种叫SSD的东西，未来三四年内将会成为某些平板电脑的硬盘。可惜的是微软那时候没有成功推广平板电脑。

从2003年开始，SSD的时代终于到来，SSD开始成为存储行业的一个热词，固态硬盘的概念开始为许多人所知晓。

2005年5月，三星电子宣布进入SSD市场，这是第一家进入这个市场的科技巨头。

5. 2006年，SSD进入笔记本

2006年，NextCom制造的笔记本开始使用SSD。三星推出了32GB的SSD，并认为2007年SSD市场容量可达13亿美金，2010年将达到45亿

美金。9月，三星推出了PRAM SSD，这另一种SSD技术，其采用了PRAM作为载体，三星希望能取代NOR闪存。

同年11月，微软的Windows Vista来到了市场上，这是第一款支持SSD特殊功能的PC操作系统。

6.2007，革命之年

2007年，Mtron和Memoright公司开发了2.5寸和3.5寸的闪存SSD，读写带宽和随机IOPS性能终于达到了最快的企业级HDD水平，同时闪存SSD开始在某些领域替代原来的RAM SSD。硬盘大战的序幕从此拉开。

2月份，Mtron推出的PATA SSD写速度为80MB/s，但是仅仅8个月后，Memoright的PATA和SATA SSD成为速度最快的——100MB/s的读写速度。

企业级市场玩家Violin Memory和Texas Memory Systems也推出了大型SSD。TMS的RamSan-500容量达2TB，DDR RAM作为缓存，闪存作为存储。随机读IOPS 100k，随机写10k，顺序读写带宽达到了惊人的2GB/s！来看看这个大家伙（见图1-10）。



图1-10 大型SSD

闪存厂商SanDisk、Micron也推出了一系列的SATA SSD，Toshiba也宣布要做SSD。年底的时候，市场上有60家SSD OEM厂商。

7.2008年，速度大战爆发

2008年，SSD厂商迅速达到了100家，就是说一年内新冒出了40家新的SSD厂商。这一年使用的闪存还是SLC。SLC虽然容量小、价格高，但是挡不住大家的热情，IOPS不断被打破。

EMC再次推出了使用SSD的网络存储系统Symmetrix DMX-4，上一次使用SSD是在20年前，不过那时候是RAM SSD。三星想要收购SanDisk，悲剧的是被拒绝了，还好Sandisk的股东脑子清醒，因为现在Sandisk已经是一家市值百亿美金的巨头（2015年SanDisk以190亿美元价格被西数收购）。Violin Memory甚至宣布他们的4TB 1010Memory Appliance可以达到4KB随机读带宽200k，随机写100k IOPS，支持PCIe、Fibre Channel和以太网接口。Fusion-IO的SSD开始为HP的BladeSystem服务器提供加速功能。

著名的OCZ公司开始进入2.5寸SSD市场。Intel开始出售X-25E 2.5寸32GB SATA SSD，读延迟75 μ s，10个通道，读写带宽分别是250/170MB/s。4KB随机读写带宽35k IOPS和3.3k IOPS。

8.2009年，SSD的容量赶上了HDD

PureSilicon公司的2.5寸SSD做到了1TB容量，由128片64Gb的MLC闪存组成。SSD终于在同样的空间内，实现了和HDD一样大的容量。这一点很重要，因为之前HDD厂商认为HDD的优势是容量增大很容易，增加盘片密度就可以了，成本很低，而SSD必须要内部芯片数量翻番才能实现容量翻倍。但是这款MLC SSD证明一个存储单元（Cell）多存几个比特也可以让容量翻几番，但是性能却远超HDD：读写带宽分别为240MB/s和215MB/s，读延迟小于100 μ s，随机读写分别为50k IOPS和10k IOPS。HDD厂商的危机来临了。

SSD的巨大革新惊动了很多人技术大牛，Apple的早期创始人Steve Wozniak成为Fusion-IO的首席科学家。

大名鼎鼎的SandForce推出了第一代SSD控制器SF-1000，是当时最快的2.5寸SATA SSD芯片，拥有250MB/s读写带宽，30k IOPS。Intel为内部员工配备了1万台SSD笔记本。Micron的C300SSD实现读带宽355MB/s和写带宽215MB/s。

在SSD的热潮中，HDD的巨头希捷也坐不住了，试验性地开始销售SSD产品。

9.2010年，SSD市场开始繁荣

2010年，SSD市场达到了10亿美金。

Fusion-IO宣布年度营收增长300%。SandForce开始使用广告词“SandForce Driven SSDs”。这一年企业级市场还是SLC，但是消费级产品开始广泛使用MLC了。

10.2011~2012年，上市、收购，群雄并起

2011年6月，Fusion-IO上市，市值18亿美金，后来一度达到40多亿美金，这家当年的明星公司没想到后来11亿美金便宜卖掉了，令人唏嘘不已，可见大家看好的SSD市场竞争异常激烈。

SandForce说他们的SSD控制器内置数据实时压缩功能，这使得SSD的使用寿命进一步延长，读写带宽也得到提高。因为经过压缩后，实际写入SSD内部的数据大幅度减少，这个实时压缩技术听起来简单，可是实现起来异常复杂，因为压缩之后每一个用户数据页的大小都不一样，映射表等的设计需要非常精妙。所以，至今仍然没有几家公司实现SSD内部压缩。不得不说，已经被轮番收购，最后落入希捷手中的SandForce是SSD控制器市场最成功的公司：做出了最成功的产品，技术非常精妙，市场又很成功。

新的厂商不断出现，巨头的土地兼并也开始了。几个著名的控制器芯片厂商消失：2011年年初，OCZ以3200万美金收购Indilinx；年底，老牌存储芯片玩家LSI以3.7亿美金收购了SandForce；2012年6月，Hynix收购了LAMD（Link A Media Devices）。

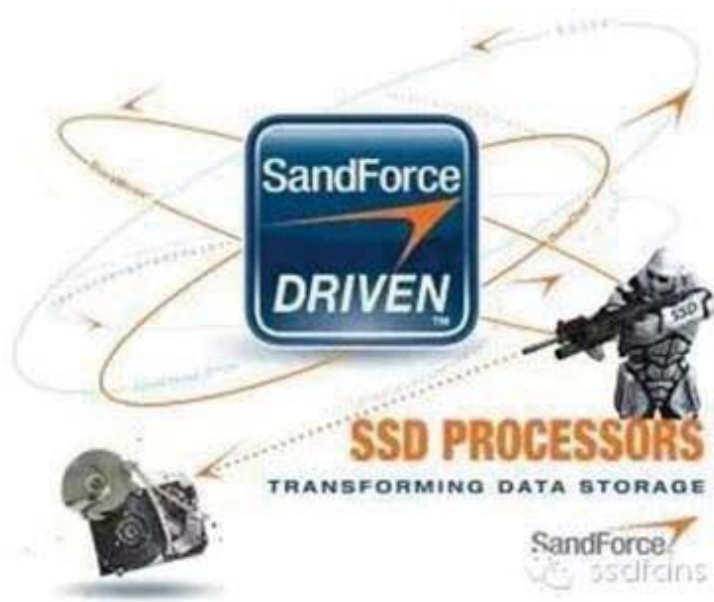


图1-11 SandForce宣传SSD击败HDD的海报

企业级市场也开始使用MLC。闪存阵列厂商Skyera（其Logo如图1-12所示）推出了44TB的SSD，售价13.1万美金！



图1-12 Skyera Logo

这一年的另一个重大事件是IBM收购了老牌RAM SSD厂商TMS。

11.2013年，PCIe SSD进入消费者市场

台式机和笔记本觉得SATA已经不够用了，SATA是为HDD设计的接口，最大速度是6Gbps，只能达到最高600MB/s的带宽（扣除协议开销，实际速度可能只有560MB/s左右），同时命令队列不够深，不适合SSD使用。SSD开始在协议上引发存储技术的变革。

同时出现了可以插在内存DIMM插槽里的SSD，容量大，速度快，掉电数据还在，就看用户怎么使用内存了。软件可得跟上啊！

闪存阵列厂商Violin Memory纳斯达克上市，让投资人悲催的是当天股价从9美金跌到7美金，两周后CEO Donald Basile被赶跑了。看来全闪存阵列的前景并不被看好。

年底，LSI被Avago以66亿美金收购。

12.2014年，SSD软件平台重构企业级存储

SSD大放异彩需要整个生态链的支持，因为以前的软件和协议都是为慢速HDD设计的。现在它们需要适应快速的硬盘。

VMware的VSAN能够支持3~8个服务器节点。SanDisk的企业级存储软件ZetaScale

支持占用大量内存的应用，有了SSD后，DRAM作为缓存，SSD来存储程序数据，速度依然很快。这对有着大量数据的数据库来说非常有用，不用开发硬盘的接口了，数据都可以放在内存里面。

SanDisk 11亿美金收购Fusion-IO，希捷4.5亿美金收购Avago (LSI) 的企业级SSD部门ASD和SSD控制器芯片部门FCD (SandForce) 。

年底，原SandForce创始团队创建的创业公司Skyera被WD收购。

13.2015年，3D XPoint

Tezarron说会在2016年采用Rambus的ReRAM来做SSD。

Northwest Logic开发的FPGA控制器可以支持Everspin的MRAM。

Toshiba发布48层3D闪存样品，容量16GB。

Diablo和Netlist打官司，Diablo赢了，官司的内容是ultrafast Flash DIMM。他们发布了Memory1，号称能在需要大内存的环境下替换内存。

不过Netlist宣布和Samsung合作开发Flash As RAM的DIMM。

SSD控制器厂商SMI 5700万美金收购了SSD厂商Shannon Systems——宝存科技。

7月，Intel和Micron宣布开发出了新型存储器——3D XPoint。

Pure Storage完成IPO，上市。

Crossbar D轮融资3500万美金，开发RRAM SSD。

WD 190亿美金收购Sandisk。

14.2016年，NVDIMM开始供货，关键是怎么标准化

Google经过测试认为不值得花那么多钱去买SLC，其实MLC性价比更高。

NVMdurance再次融资，号称能延长闪存寿命。

Cadence和Mellanox展示了PCIe 4.0技术，带宽达到16Gbps。

Pure Storage表示2016年第一季度全闪存阵列收入超过了机械硬盘阵列头号厂商。

Diablo的128GB DDR4Memory1开始供货。

希捷展示60TB的3.5寸SAS SSD。

Nimbus在FMS上展示4PB 4U HA全闪存阵列。

Everspin（MRAM）启动上市IPO进程。

Rambus宣布了基于FPGA的数据加速卡项目。

SiliconMotion发布了世界上第一颗SD 5.1标准的SD卡控制器。

Violin破产保护。

1.4 SSD基本工作原理

从主机PC端开始，用户从操作系统应用层面对SSD发出请求，文件系统将读写请求经驱动转化为相应的符合协议的读写和其他命令，SSD收到命令执行相应操作，然后输出结果，每个命令的输入和输出经协议标准组织标准化，这是标准的东西，和HDD无异，只不过HDD替换成SSD硬件存储数据，访问的对象变成SSD。

SSD的输入是命令（Command），输出是数据（Data）和命令状态（Command Status）。SSD前端（Front End）接收用户命令请求，经过内部计算和处理逻辑，输出用户所需要的数据或状态。

从图1-13所示可以看出，SSD主要有三大功能模块组成：

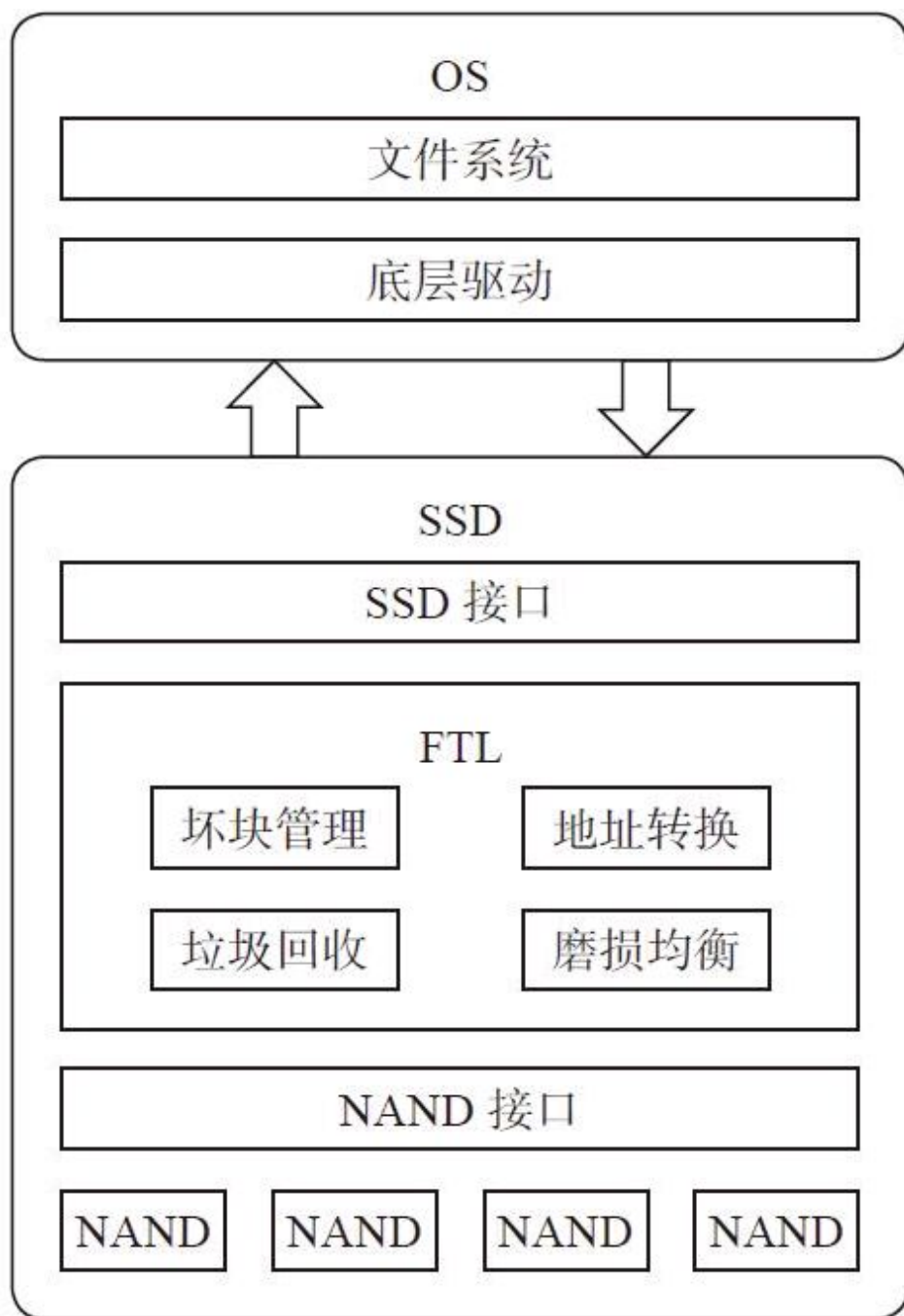


图1-13 SSD系统调用

- 前端接口和相关的协议模块；
- 中间的FTL层（Flash Translation Layer）模块；
- 后端和闪存通信模块。

SSD前端负责和主机直接通信，接收主机发来的命令和相关数据，命令经SSD处理后，最终交由前端返回命令状态或数据给主机。SSD通过诸如SATA、SAS和PCIe等接口与主机相连，实现对应的ATA、SCSI和NVMe等协议，如表1-5所示。

表1-5 SATA/SAS/PCIe接口协议

接口	协议命令	主机控制器接口	标准组织
SATA	ATA/SATA 命令集	AHCI (Advanced Host Controller Interface)	ATA-IO
SAS	SCSI 命令集	SCSI	T10 of INCITS
PCIe	NVMe 命令集	NVMe	PCIExpress/NVM Express

我们看看SSD是怎么进行读写的，以写为例。

主机通过接口发送写命令给SSD，SSD接收到该命令后执行，并接收主机要写入的数据。数据一般会先缓存在SSD内部的RAM中，FTL会为每个逻辑数据块分配一个闪存地址，当数据凑到一定数量后，FTL便会发送写闪存请求给后端，然后后端根据写请求，把缓存中的数据写到对应的闪存空间。

由于闪存不能覆盖写，闪存块需擦除才能写入。主机发来的某个数据块，它不是写在闪存固定位置，SSD可以为其分配任何可能的闪存空间写入。因此，SSD内部需要FTL这样一个东西，完成逻辑数据块到闪存物理空间的转换或者映射。

举个例子，假设SSD容量为128GB，逻辑数据块大小为4KB，所以该SSD一共有 $128\text{GB}/4\text{KB}=32\text{M}$ 个逻辑数据块。每个逻辑块都有一个映射，即每个逻辑块在闪存空间都有一个存储位置。闪存地址大小如果用4字节表示，那么存储32M个逻辑数据块在闪存中的地址则需要 $32\text{M}\times4\text{B}=128\text{MB}$ 大小的映射表。

正因为SSD内部维护了一张逻辑地址到物理地址转换的映射表，当主机发来读命令时，SSD能根据需要读取的逻辑数据块查找该映射表，获取这些逻辑数据在闪存空间所在的位置，后端便能从闪存上把对应数据读到SSD内部缓存空间，然后前端负责把这些数据返回给主机。

由于前端接口协议都是标准化的，后端和闪存的接口及操作也是标准化的（闪存遵循ONFI或者Toggle协议），因此，一个SSD在前端

协议及闪存确定下来后，差异化就体现在FTL算法上了。FTL算法决定了性能、可靠性、功耗等SSD的核心参数。

其实，FTL除了完成逻辑数据到闪存空间的映射，还需要做很多其他事情。

前面提到，闪存不能覆盖写，因此随着用户数据的不断写入，闪存空间会产生垃圾（无效数据）。FTL需要做垃圾回收（Garbage Collection），以腾出可用闪存空间用以写用户数据。

以图1-14所示为例，在Block x和Block y上有很多垃圾数据，其中Block x上的A、B、C为有效数据，Block y上的D、E、F、G为有效数据。垃圾回收就是把一个或者几个Block上的有效数据搬出来集中写到某个空闲Block上（比如Block z）。当这些Block上的有效数据都搬走后，FTL便能擦除这些Block，然后又能把这些Block拿出来供SSD写入新的数据了。

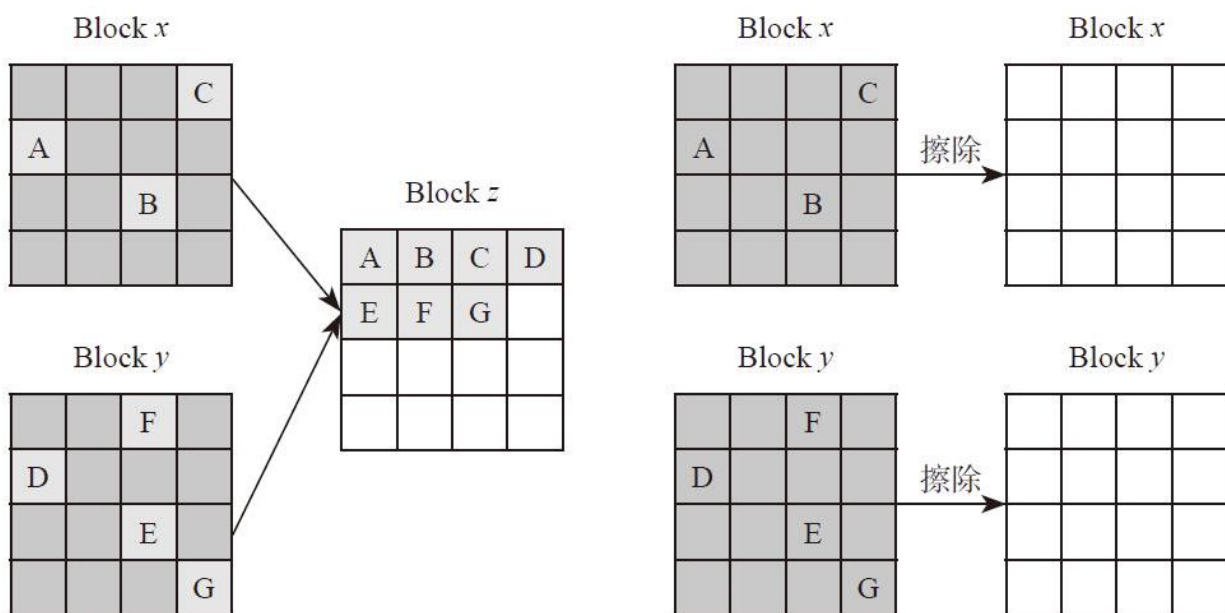


图1-14 垃圾数据回收

还有，闪存都是有寿命的，每个闪存块不能一直写数据，因此，为保证最大的数据写入量，FTL必须尽量让每个闪存块均衡写入，这就是磨损平衡（Wear Leveling）。

除此之外，FTL还需要实现坏块管理、读干扰处理、数据保持处理、错误处理等很多其他事情。理解了FTL，SSD的工作原理也就掌握了。关于FTL，本书有专门章节介绍，读者可自行跳到第4章阅读。

1.5 SSD产品核心参数

用户在购买SSD之前，会关注它的一些参数指标，比如能跑多快、用的是什么闪存等。特别是企业级用户，需要全方位研究SSD的核心指标，解决关注什么指标、如何关注、竞争产品对比等问题，最终逐一拨开产品内在本质。本节以Intel一款企业级SATA接口数据中心盘S3710SSD产品手册为例（见图1-15），带大家一起解读SSD产品的核心参数。

Intel® Solid-State Drive DC S3710 Series

Product Specification

- Capacity:
 - 200GB, 400GB, 800GB, 1.2TB
- Components:
 - Intel® 20nm NAND Flash Memory
 - High Endurance Technology (HET)
 - Multi-Level Cell (MLC)
- Form Factor: 2.5-inch
- Read and Write IOPS^{1,2}
(Full LBA Range, IOMeter® Queue Depth 32)
 - Random 4KB³ Reads: Up to 85,000 IOPS
 - Random 4KB Writes: Up to 45,000 IOPS
 - Random 8KB³ Reads: Up to 52,000 IOPS
 - Random 8KB Writes: Up to 21,000 IOPS
- Bandwidth Performance¹
 - Sustained Sequential Read: Up to 550 MB/s⁴
 - Sustained Sequential Write: Up to 520 MB/s
- Endurance: 10 drive writes per day⁵ for 5 years
 - 200GB: 3.6PB 400GB: 8.3PB
 - 800GB: 16.9PB 1.2TB: 24.3PB
- Latency (average sequential)
 - Read: 55 µs (TYP)
 - Write: 66 µs (TYP)
- Quality of Service^{6,8}
 - Read/Write: 500 µs / 5 ms (99.9%)
- Performance Consistency^{7,8}
 - Read/Write: Up to 90%/90% (99.9%)
- AES 256-bit Encryption
- Altitude⁹
 - Operating: -1,000 to 10,000 ft
 - Operating¹⁰: 10,000 to 15,000 ft
 - Non-operating: -1,000 to 40,000 ft
- Product Ecological Compliance
 - RoHS*
- Compliance
 - SATA Revision 3.0; compatible with SATA 6Gb/s, 3Gb/s and 1.5Gb/s interface rates
 - ATA/ATAPI Command Set – 2 (ACS-2 Rev 7); includes SCT (Smart Command Transport) and device statistics log support
 - Enhanced SMART ATA feature set
 - Native Command Queuing (NCQ) command set
 - Data set management Trim command
- Power Management
 - 5V or 5V+12V SATA Supply Rail¹¹
 - SATA Interface Power Management
 - OS-aware hot plug/removal
 - Enhanced power-loss data protection feature
- Power¹²
 - Active: Up to 6.9 W (TYP)⁸
 - Idle: 600 mW
- Weight:
 - 200GB: 82 grams ± 2 grams
 - 400GB: 82 grams ± 2 grams
 - 800GB: 88 grams ± 2 grams
 - 1.2TB: 94 grams ± 2 grams
- Temperature
 - Operating: 0° C to 70° C
 - Non-Operating¹³: -55° C to 95° C
 - Temperature monitoring and logging
 - Thermal throttling
- Shock (operating and non-operating): 1,000 G/0.5 ms
- Vibration
 - Operating: 2.17 G_{RMS} (5-700 Hz)
 - Non-Operating: 3.13 G_{RMS} (5-800 Hz)
- Reliability
 - Uncorrectable Bit Error Rate (UBER): 1 sector per 10¹⁷ bits read
 - Mean Time Between Failures (MTBF): 2 million hours
 - End-to-End data protection
- Certifications and Declarations
 - UL*, CE*, C-Tick*, BSMI*, KCC*, Microsoft® WHCK, VCCI*, SATA-IO*
- Compatibility
 - Windows 7* and Windows 8*, and Windows 8.1*
 - Windows Server 2012* R2
 - Windows Server 2012*
 - Windows Server 2008* Enterprise 32/64bit SP2
 - Windows Server 2008* R2 SP1
 - Windows Server 2003* Enterprise R2 64bit SP2
 - VMWare* 5.1, 5.5
 - Red Hat* Enterprise Linux* 5.5, 5.6, 6.1, 6.3, 7.0
 - SUSE* Linux* Enterprise Server 10, 11 SP1
 - CentOS* 64bit 5.7, 6.3
 - Intel® SSD Toolbox with Intel® SSD Optimizer

图1-15 Intel DC S3700固态硬盘规格书截图

从图1-15所示分类来看，这份文档给用户展示了SSD几大核心参数：

·基本信息：包括容量配置（Capacity）、介质信息（Component）、外观尺寸（Form Factor）、重量（Weight）、环境温

度（Temperature）、震动可靠性（Shock和Vibration）、认证（Certifications）、加密（Encryption）等信息。

·性能指标：连续读写带宽、随机读写IOPS、时延（Latency）、最大时延（Quality of Service）。

·数据可靠性和寿命：Reliability、Endurance。

·功耗：Power Management、Active Power和Idle Power。

·兼容性等：Compliance、Compatibility（与操作系统集成时参考）。

当然，还有其他一些重要信息在产品规范书里是无法体现出来的，比如产品可靠性（RMA Rate）。由于固件或者硬件缺陷导致产品返修率高低是很关键的，在保质期内产品返修率越低越好。尤其是企业级硬件，数据比SSD盘本身更重要，用户不能容忍的是由于固件、硬件可靠性问题或缺陷导致丢数据，或者数据无法通过技术手段恢复。

产品的测试条件信息、产品的系统兼容性好坏的信息等也是无法在产品规范书里体现出来的。这些也是考验购买SSD的用户对SSD理解的深度。从测试条件的苛刻设计中提炼出用户自己想要的测试用例，用测试结果来反映产品规范书里无法透露和显示的产品的实际数据信息。当然，能通过苛刻的测试，并在实际上线运行中经受住系统的考验，日积月累，产品的品牌就打出来了。每家SSD OEM客户都有自己的标准和测试，通过实际测试和运行数据检验出口碑和质量好或差的SSD供应商。

行业是公平的，长期来看，对于各供应商的SSD质量客户心中是有数的。

1.5.1 基本信息剖析

1.SSD容量

SSD容量是指提供给终端用户使用的最终容量大小，以字节（Byte）为单位。这里要注意，标称的数据都以十进制为单位的，程序员出身的人容易把它当成二进制。同样一组数据，二进制比十进制会多出7%的容量，例如：

十进制128GB： $128 \times 1000 \times 1000 \times 1000 = 128000000000$ 字节

二进制128GB： $128 \times 1024 \times 1024 \times 1024 = 137438953472$ 字节

以二进制为单位的容量行业内称为裸容量，以十进制为单位的容量称为用户容量。

裸容量比用户容量多出7%。这里指GB级，当进入到TB级时，数值差距更大。读者可自行计算。

对于闪存本身，它是裸容量。那么，裸容量多出的7%容量在SSD内部做什么用呢？SSD可以利用这多出来的7%空间管理和存储内部数据，比如把这部分额外的空间用作FTL映射表存储空间、垃圾回收所需的预留交换空间、闪存坏块的替代空间等。这里的7%多余空间也可以转换为OP概念（Over Provisioning），公式是：

$$OP = \frac{\text{SSD 裸容量} - \text{用户容量}}{\text{用户容量}}$$

2.介质信息

当前SSD盘核心存储介质是闪存，闪存这种半导体介质有其自身物理参数，例如寿命（PE cycles，编程擦除次数）、Program（写编程）、Erase（擦除）和Read（读）时间、温度对读写擦的影响、闪存页的大小、闪存块的大小.....这些都是介质的信息，介质的好坏直接影响数据存储的性能和完整性。

闪存分SLC、MLC、TLC（甚至QLC），它指的是一个存储单元存储的比特数（见表1-6）：

表1-6 SLC、MLC和TLC参数比较

闪存类型	SLC	MLC	TLC
每单元比特数	1	2	3
擦除次数 (k)	100	3	1
读取时间 (μs)	30	50	75
编程时间 (μs)	300	600	1 000
擦除时间 (μs)	1 500	3 000	4 500

·SLC（Single-Level Cell）即单个存储单元存储1bit的数据。SLC速度快，寿命长（5万~10万次擦写寿命），但价格超贵（约是MLC 3倍以上的价格）。

·MLC（Multi-Level Cell）即单个存储单元存储2bit的数据。MLC速度一般，寿命一般（约为3k~10k次擦写寿命），价格一般。

·TLC（Trinary-Level Cell）即单个存储单元存储3bit的数据，也有闪存厂家叫8LC，速度慢，寿命短（约500~1500次擦写寿命），价格便宜。

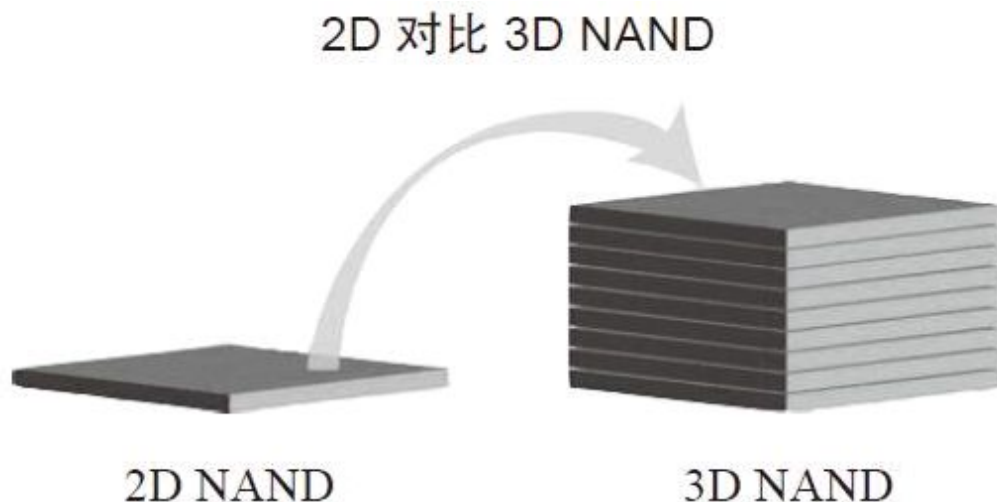


图1-16 2D vs.3D闪存结构示意图

闪存发展到现在，经历了2D平面到现在的3D立体制程（Process）的大发展，目标只有一个：硅片单位面积（ mm^2 ）能设计生产出更多的比特（bit），让每GB成本和价格更低。这是介质厂商的目标和客户的诉求，同时也是半导体工业发展的趋势。

来看一下2D到3D的单位面积比特数的比较（见表1-7），48层Samsung的3D V-NAND每平方毫米能生产出2600Mb的数据，3倍于2D闪存，所以同样的晶圆可以切割3倍的数据量，简单计算的话每GB的价格能降为原来的1/3。

表1-7 不同闪存密度对比

	Micron 16 nm	Hynix 16 nm	Samsung 16 nm	Samsung 48L V-NAND
年份	2014	2014	2015	2016
制程节点 (nm)	16	16	16	21
Die 容量 (Gb)	128	64	64	256
Die 面积 (mm^2)	176	93	86.4	99
密度 (Mb/mm^2)	730	690	740	2 600

最后我们来看一下各家闪存生产发展节点图（见图1-17），若一句话来概括最终竞争的目标，则为：在制程允许的范围内，发展更密、更快、价格更低的闪存产品。

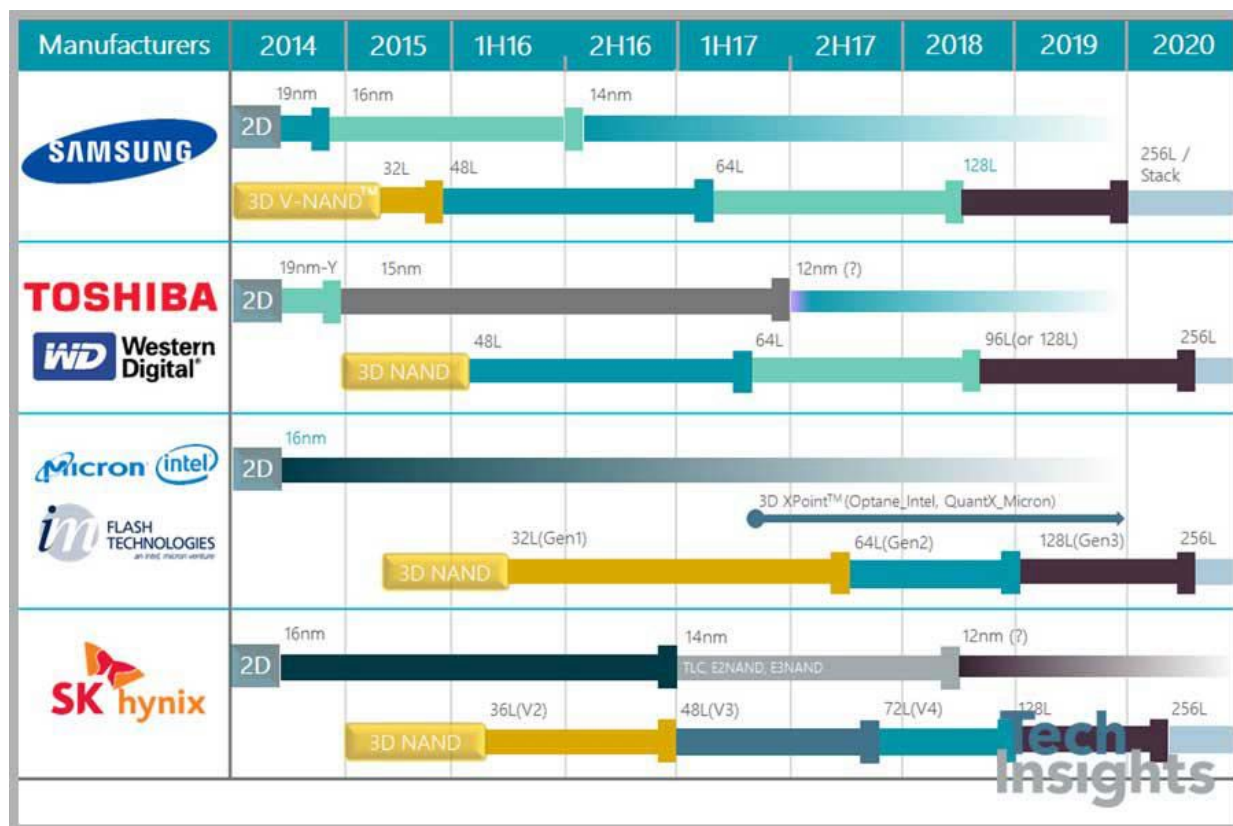


图1-17 闪存原厂路线图

3.外观尺寸

SSD是标准件，外观尺寸需要满足一定的规定要求（长宽高和接口连接器），这又通常称为Form Factor。那SSD会有哪些Form Factor呢？细分为3.5寸、2.5寸、1.8寸、M.2、PCIe card、mSATA、U.2等Form Factor标准（见图1-18），每个Form Factor也都有三围大小、重量和接口引脚等明确规范。

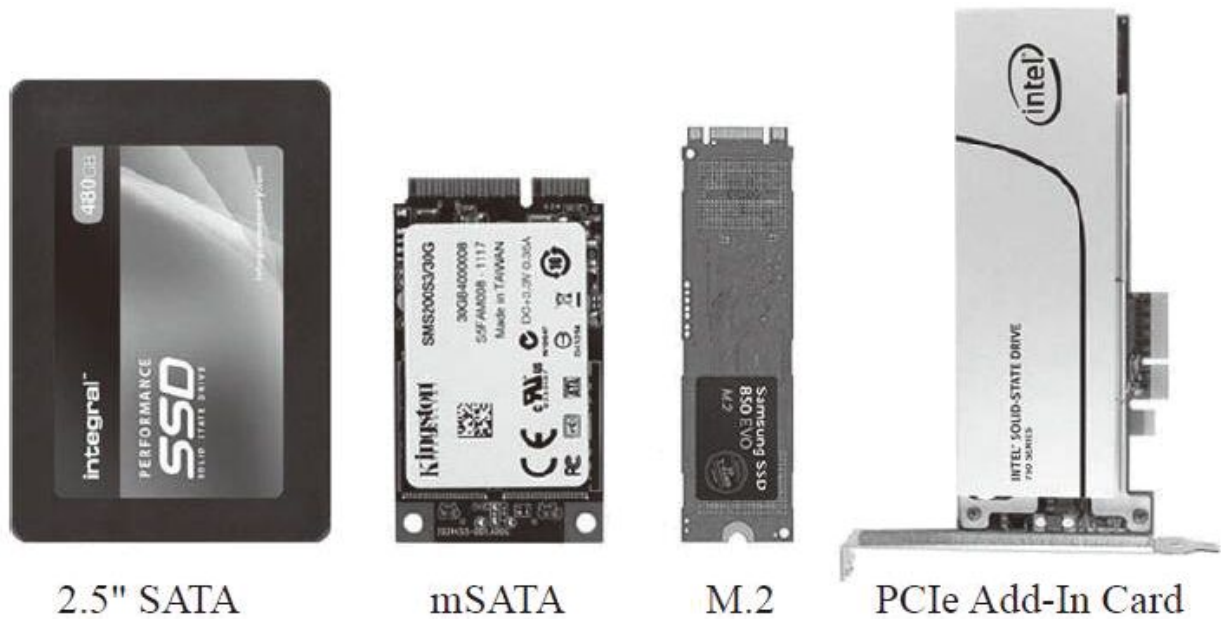


图1-18 SSD尺寸部分一览

Form Factor标准组织:

- <https://www.snia.org/forums/sssi/knowledge/formfactors>
- <http://www.ssdformfactor.org/>

4.其他

我们这里看看温度和认证及兼容性信息这两个参数。

·温度: 所有工业品都有温度规范, SSD应在一定温度范围内使用。工作温度为 $0^{\circ}\text{C} \sim 70^{\circ}\text{C}$, 说的是SSD在运行状态时的温度, 超出这个温度范围SSD可能出现产品异常和数据异常, 这不在产品保证和保修范围内。非工作温度为 $-50^{\circ}\text{C} \sim 90^{\circ}\text{C}$, 这是SSD储存和运输期间的温度, 也就是在非开机工作状态下, 产品运输和仓库存储时的参考温度参考。超出 $-50^{\circ}\text{C} \sim 90^{\circ}\text{C}$, SSD可能会发生损坏。

·认证及兼容性信息(见图1-19): SSD硬件和软件都应通过一定认证测试来反映产品的标准测试情况, 从而让客户明确是不是过了相应的测试。认证和兼容性是对应标准组织的测试集, 标准组织属于第三方, 独立客观, 测试通过意味着可以免去客户一部分测试。

- Certifications and Declarations
 - UL*, CE*, C-Tick*, BSMI*, KCC*, Microsoft* WHCK, VCCI*, SATA-IO*
- Compatibility
 - Windows 7* and Windows 8*, and Windows 8.1*
 - Windows Server 2012* R2
 - Windows Server 2012*

图1-19 SSD兼容性示例

1.5.2 性能剖析

1.性能指标

硬盘性能指标一般包括IOPS（Input Output Operations Per Second，反映的是随机读写性能）、吞吐量（Throughput，单位MB/s，反映的是顺序读写性能）、Response Time/Latency（响应时间/时延，单位ms或 μ s）。

·IOPS：单位IOPS，即设备每秒完成IO请求数，一般是小块数据读写命令的响应次数，比如4KB数据块尺寸。IOPS数字越大越好。

·吞吐量：单位MB/s，即每秒读写命令完成的数据传输量，也叫带宽（Bandwidth），一般是大块数据读写命令，比如512KB数据块尺寸。吞吐量越大越好。

·响应时间：也叫时延（Latency），即每个命令从发出到收到状态回复所需要的响应时间，时延指标有平均时延（Average Latency）和最大时延两项（Max Latency）。响应时间越小越好。

2.访问模式

性能测试设计上要考虑访问模式（Access Pattern），包括以下三部分：

·Random/Sequential：随机（Random）和连续（Sequential）数据命令请求。何为随机和连续？指的是前后两条命令LBA地址是不是连续的，连续的地址称为Sequential，不连续的地址称为Random。

·Block Size：块大小，即单条命令传输的数据大小，性能测试从4KB~512KB不等。随机测试一般用小数据块，比如4KB；顺序测试一般用大块数据，比如512KB。

·Read/Write Ratio：读写命令数混合的比例。

任何测试负荷（workload）都是这些模式的组合，比如：

1) 顺序读测试：指的是LBA连续读，块大小为256KB、512KB等大尺寸数据块，读写比例为100%: 0；

2) 随机写测试：指的是LBA不连续的写，块大小一般为4KB，读写比例为0: 100%；

3) 随机混合读写：指的是LBA不连续的读写混合测试，块大小一般为4KB，读写保持一定的比例。

3.时延指标

时延有平均时延和最大时延，数值越低越好。平均时延计算公式是整个应用或者测试过程中所有命令响应时间总和除以命令的个数，反映的是SSD总体平均时延性能；最大时延取的是在测试周期内所有命令中响应时间最长的那笔，反映的是用户体验，例如最大时延影响应用通过操作系统操作SSD时有无卡顿的用户体验。时延上了秒级，用户就会有明显的卡顿感知。

4.服务质量指标

服务质量（Quality of Service, QoS）表达的是时延“置信级”（Confidence Level），如图1-20所示，在测试规定的时间内使用2个9（99%）到5个9（99.999%）的百分比的命令中最大的时延（Max Latency），也就是最慢的那条命令的响应时间。整体上看，一个SSD盘QoS时延分布整体越靠左越好，即时延越小越好。

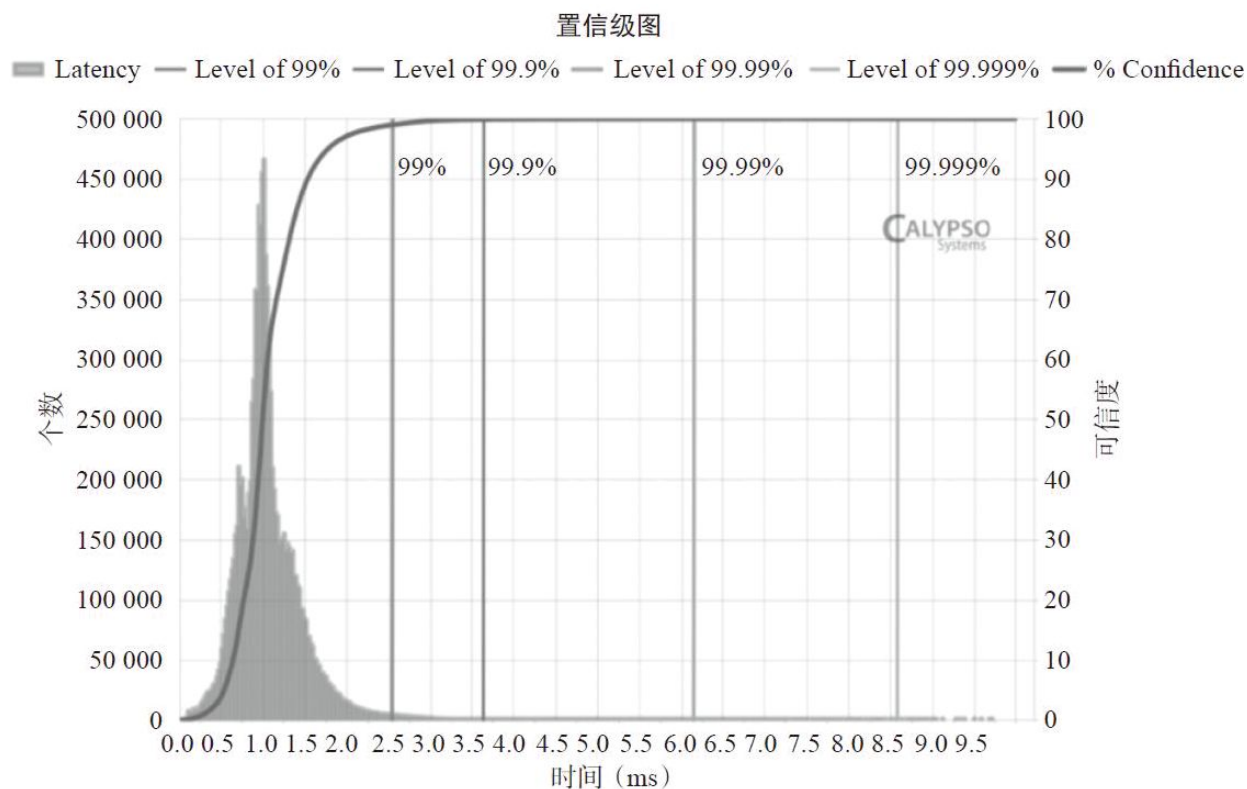


图1-20 SSD时延分布图

对消费级硬盘来说，用户对时延要求可能不是很高。但对企业级硬盘来说，像数据中心（Data Center）等企业应用对时延的要求很敏感，比如BAT（百度、阿里巴巴、腾讯）的互联网应用，时延的大小关乎用户体验和互联网应用快慢的问题。这种类型的应用对IOPS和吞吐量并不十分敏感，而更在乎时延（包括平均时延、最大时延或服务质量等指标）。

5.性能数据一览

我们来看一组性能测试数据，包括SSD、HDD和SSHD（SSD和HDD混合硬盘）的性能数据，如图1-21所示。

SSD, HDD 和 SSHD 性能数据总结									
级别	种类	空盘 IOPS	IOPS (数字越大越好)				吞吐量 (数字越大越好)		响应时间 (越快越好)
存储设备	Form Factor, Capacity, Cache	RND 4KB 100% W	RND 4KB 100% W	RND 4KB 65:35 RW	RND 4KB 100% R	SEQ 1024KB 100% W	SEQ 1024KB 100% R	RND 4KB 100% W AVE	RND 4KB 100% W MAX
HDD 和 SSHD									
7 200 RPM SATA Hybrid R30-4	2.5" SATA 500 GB WCD	125	147	150	135	97 MB/s	99 MB	15.55 msec	44.84 msec
15 000 RPM SAS HDD IN-1117	2.5" SAS 80 GB WCD	350	340	398	401	84 MB/s	90 MB/s	5.39 msec	97.28 msec
消费级 SSDs									
SATA 3 SSD R32-336	mSATA 32 GB WCD	18 000	838	1 318	52 793	79 MB/s	529 MB/s	1.39 msec	75.57 msec
SATA 3 SSD IN8-1025	SATA3 256 GB WCD	56 986	3 147	3 779	29 876	240 MB/s	400 MB/s	0.51 msec	1 218.45 msec
SATA 3 SSD R30-5148	SATA3 256 GB WCE	60 090	60 302	41 045	40 686	249 MB/s	386 MB/s	0.35 msec	17.83 msec
企业级 SSDs									
Enterprise SAS SSD RI-2288	SAS 400 GB WCD	61 929	24 848	29 863	53 942	393 MB/s	496 MB/s	0.05 msec	19.60 msec
Server PCIe SSD INI-1727	PCIe 320 GB WCD	133 560	73 008	53 797	54 327	663 MB/s	772 MB/s	0.05 msec	12.60 msec
Server PCIe SSD IN24-1349	PCIe 700 GB WCD	417 469	202 929	411 390	684 284	1 343 MB/s	2 053 MB/s	0.03 msec	0.58 msec

图1-21 SSD、HDD和SSHD性能数据一览

测量指标包括空盘（FOB，Fresh out of Box）和满盘下的IOPS、吞吐量、平均时延和最大时延。

测试空盘IOPS用的测试模式是“RND 4KB 100%W”，即4KB（二进制4KB，即4096字节）随机100%纯写。

测试满盘下IOPS，用了三种测试模式，分别为：

1) RND 4KB 100%W：数据块大小为4KB的写命令，100%随机写；

2) RND 4KB 65: 35RW: 数据块大小为4KB的读写命令，65%的读，35%的写，混合随机读写；

3) RND 4KB 100%R: 数据块大小为4KB的读命令，100%随机读。

从图1-21中我们可以看出，对HDD和SSHD，满盘下和空盘下写的IOPS相差不大（都很糟糕），而对SSD来说，满盘和空盘写的IOPS相差很大。这是因为，对HDD来说，满盘后，没有垃圾回收操作，所以空盘和满盘下写的性能差不多；但对SSD来说，满盘后，写会触发垃圾回收，导致写性能下降。

对消费级SSD来说，商家给的测试数据一般是空盘下测试的数据，数字相当好看，“最高可达”常挂嘴边。新买的盘，我们测试时会发现性能和商家标称的差不多，但随着盘的使用，会出现掉速问题。垃圾回收是其中一个原因，还有可能就是SLC缓存用完了，这里就不具体展开了。

对企业级SSD来说，客户更关注的是稳态性能，即满盘性能。所以，商家给出的性能参数一般是满盘数据，“最高可达”字眼消失。我们可以从有没有“最高可达”来快速判断一个盘是企业级还是消费级。

关于吞吐量测试，有两种模式，分别为：

1) SEQ 1024KB 100%W: 数据块大小为1024KB的顺序写测试；

2) SEQ 1024KB 100%R: 数据块大小为1024KB的顺序读测试。

关于时延，如前所述，有平均时延和最大时延两种，其中最大时延反映的是服务质量。测试模式都是4KB 100%随机写。从上可以看出，SSD测试的是cache on下的时延，即数据到SSD的内部缓冲区即返回命令状态。为什么不是FUA？因为对闪存来说，即使是SLC，也没有办法做到几十微秒就能写入到闪存。如果是FUA命令测试的话，其平均时延至少是几百微秒。

1.5.3 寿命剖析

用户拿到一款SSD，除了关心其容量和性能参数外，还会关心它的寿命（Endurance）指标，也就是在SSD产品保质期内，总的寿命是多少，能写入多少字节的数据量。衡量SSD寿命主要有两个指标，一是DWPD（Drive Writes Per Day），即在SSD保质期内，用户每天可以把盘写满多少次；另一指标是TBW（Terabytes Written），在SSD的生命周期内可以写入的总的字节数。

1.DWPD

回头看一下上面的S3710SSD的Endurance项：

■ Endurance: 10 drive writes per day ⁵ for 5 years			
– 200GB:	3.6PB	400GB:	8.3PB
– 800GB:	16.9PB	1.2TB:	24.3PB

200GB SSD五年使用期限内对应的寿命是3600TB，平均到每天可以写入3600TB/（5×365）=1972GB，这块盘本身200GB，1972GB相当于每天写入10次，也就是规范书说的10Drive Writes Per Day，简称10DWPD。DWPD为5年的寿命期内每天可以满盘写入的次数。

由上可以看出，总的写入量可以换算成DWPD，一些SSD指标上更多使用DWPD作为寿命参数。这里要特别说明的是，从应用的角度出发，多数应用读多写少，少数应用写多读少，应用不同，对SSD的寿命要求也不同。所以我们可以将其归类为：写密集（Write Intensive）和读密集（Read Intensive）两种类型。

表1-8比较好地归纳出应用场合和应用读写特点所需求的DWPD参数，这里就不展开解释了。

表1-8 DWPD参数

用户场景	需求寿命, DWPD	成本	应用
写密集	10 ~ 25	¥¥¥	关键应用：数据库、媒体编辑、虚拟化
一般读密集	3 ~ 10	¥¥	读写差不多的应用：数据仓库、读缓存
重度读密集	1 ~ 3	¥	写少读多应用：启动分区、网页或文件服务器、视频播放

天下没有免费的午餐，DWPD越大，单盘价格自然越高。所以用户需要思考的是什么应用场景使用SSD，以及使用哪种DWPD寿命的SSD，照顾性能和经济的双重平衡。最好的平衡艺术就是根据用户数据的生存期及热度分层，或者在技术架构上根据数据冷热和存在时间为数据打标签，然后放入对应的层级以及不同DWPD的SSD。

以下是一个典型的应用场景的SSD分级应用，OLTP（联机事务处理）有大量写应用的数据（术语叫热数据），性能要求极高，所以放入T1-WI SSD层，这一层SSD单盘价格高，总容量低；第二层是写少读多应用（术语叫温数据），性能要求也很高，所以使用T2-RI SSD存放数据；第三层基本上是冷数据，极少被读到和写到，所以用大容量低价的HDD也无可厚非。总体来说OLTP用到了40%的SSD，算是对SSD需求量比较高的应用类型。当然也有不太需要SSD的应用，如图1-22最右列所示的Disaster Recovery（容灾备份）。

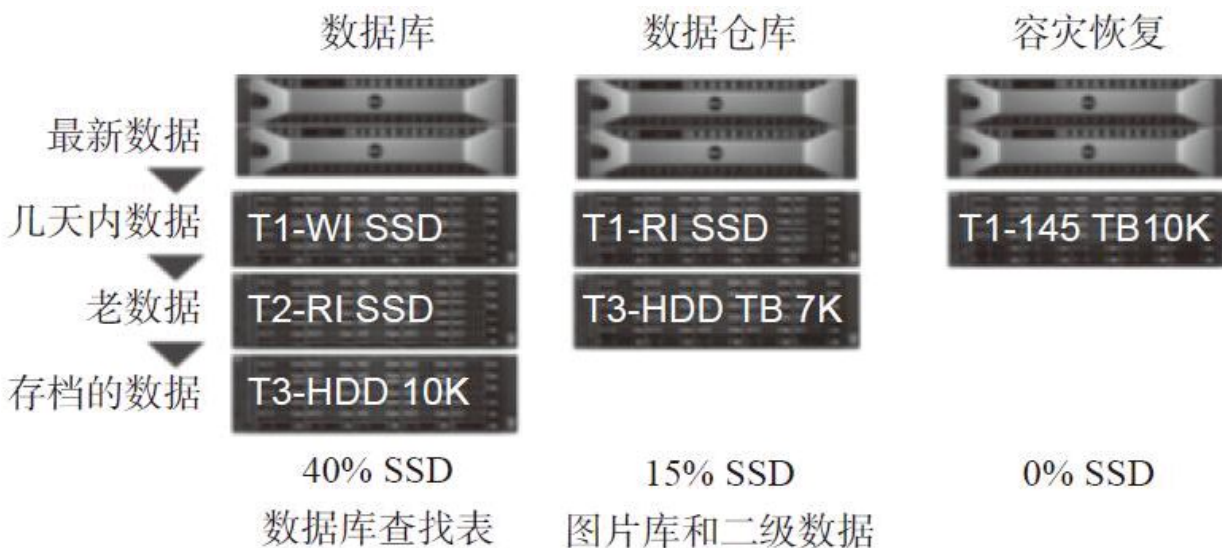


图1-22 数据分层及SSD应用

最后我们来看一下现实世界对SSD的DWPD要求。数据显示更多的应用是写少读多，83%的应用使用少于1DWPD的SSD。想象一下消费级SSD，我们每天的数据写入量是极少的，盘生命周期内几乎不会被填

满，所以极低的DWPD是可以接受的。业界主流的消费级SSD DWPD是0.3。可以预见的是，数据爆炸的时代，用户对数据总量的需求是逐年递增的，即新增数据成倍数逐年增加，尤其是企业级应用，这个83%是否会减少？答案是肯定的。

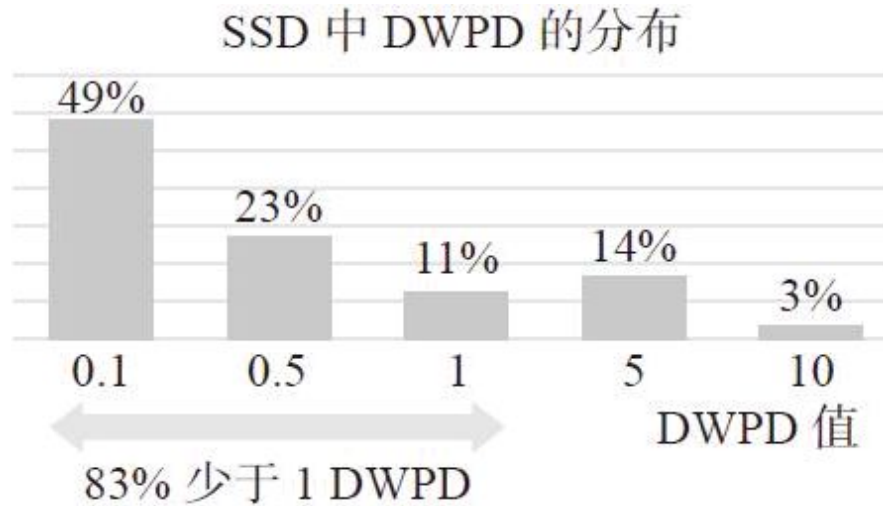


图1-23 SSD DWPD现实需求

2.TBW

TBW就是在SSD的生命周期内可以写入的总的字节数，用来表达SSD的寿命指标。从SSD的设计来看，如何设计来满足SSD的TBW要求或者SSD的TBW是如何计算的？哪些因素会影响SSD的TBW？

先给一个公式：

$$\text{总写入量TBW} = \text{Capacity (单盘容量)} \times \frac{\text{NAND PE Cycles (NAND 写擦除寿命)}}{\text{WA (写放大)}}$$

式中：

- NAND PE Cycles: SSD使用的闪存标称写擦除次数，如3K、5K。
- Capacity: SSD单盘用户可使用容量。
- WA: 写入放大系数，这跟SSD FW的设计和用户的写入的数据类型（顺序写还是随机写）强相关。

TBW和DWPD的计算公式:

$$DWPD = \frac{TBW}{\text{Years (SSD 盘标称使用年限)} \times 365 \times \text{Capacity (单盘容量)}}$$

有了上面的公式，你可以简单计算一块SSD盘的TBW或者由TBW计算每天的写入量。

1.5.4 数据可靠性剖析

SSD有几个关键指标来衡量其可靠性：UBER、RBER和MTBF。

·UBER: Uncorrectable Bit Error Rate，不可修复的错误比特率。

·RBER: Raw Bit Error Rate，原始错误比特率。

·MTBF: Mean Time Between Failure，平均故障间隔时间。

1.数据可靠性

我们接着看一下S3710SSD手册中Reliability（可靠性）项的截图：

■ Reliability

- Uncorrectable Bit Error Rate (UBER):
1 sector per 10^{17} bits read
- Mean Time Between Failures (MTBF): 2 million hours
- End-to-End data protection

UBER是一种数据损坏率衡量标准，等于在应用了任意特定的错误纠正机制后依然产生的每比特读取的数据错误数量占总读取数量的比例（概率）。

为什么SSD要定义UBER？任何一项存储设备产品，包括HDD，用户最关心的都是数据保存后的读取正确性。试想数据丢失和损坏对客户产生的后果是怎么样的？尤其是企业级用户数据。那如何让用户相信存储设备系统是可靠的呢？UBER指标描述的是出现数据错误的概率，给用户以直观的概率数据以描述错误数据出现的可能性，当然该指标越低越好。

为什么会产生错误数据？SSD的存储介质是闪存，闪存有天然的数据比特翻转率。主要有以下几种原因导致：

·擦写磨损（P/E Cycle）。

- 读取干扰（Read Disturb）。
- 编程干扰（Program Disturb）。
- 数据保持（Data Retention）发生错误。

虽然SSD主控和固件设计会用纠错码（ECC）的方式（可能还包括其他方式，如RAID）来修正错误数据，但错误数据在某种条件下依然有纠不回来的可能，所以需要UBER让用户知道数据误码纠不回来的概率。

闪存原始的数据比特翻转加上BCH码（一种ECC纠错算法）经ECC校验码保护后，可以计算转换到UBER。影响UBER最核心的因素是RBER。图1-24所示为从RBER、ECC编码长度（Code Length）和保护强度（Strength）换算到UBER，从中得出结论：相同的ECC编码长度，随着保护强度的增长，UBER在大幅度降低。

编码长度	RBER	纠错强度	码率	UBER
8192	1.25e-3	37	0.937	1.016e-13
8192	1.25e-3	38	0.935	2.705e-14
8192	1.25e-3	39	0.933	7.012e-15
8192	1.25e-3	40	0.932	1.775e-15
8192	1.25e-3	41	0.930	4.383e-16
8192	1.25e-3	42	0.928	1.057e-16
8192	1.25e-3	43	0.927	2.489e-17

↓ 4000x

图1-24 UBER和纠错强度的关系

在相同的ECC编码长度和保护强度下，RBER越低，UBER越低，并呈指数级降低，如图1-25所示。

RBER反映的是闪存的质量。所有闪存出厂时都有一个RBER指标，企业级闪存和消费级闪存的RBER显然是不同的，价格当然也有所不同。RBER指标也不是固定不变的，如图1-26所示，闪存的数据错误

率会随着使用寿命（PE Cycle）的增加而增加。为了挑战极限，必须准备好处理每100个bit就有1个坏bit的情况。

编码长度	RB ER	纠错强度	码率	UB ER
8192	2.75e-3	40	0.932	1.503e-06
8192	2.50e-3	40	0.932	2.116e-07
8192	2.25e-3	40	0.932	1.987e-08
8192	2.00e-3	40	0.932	1.128e-09
8192	1.75e-3	40	0.932	3.373e-11
8192	1.50e-3	40	0.932	4.350e-13
8192	1.25e-3	40	0.932	1.775e-15

↓ 840 000 000x

图1-25 UBER和RBER的关系

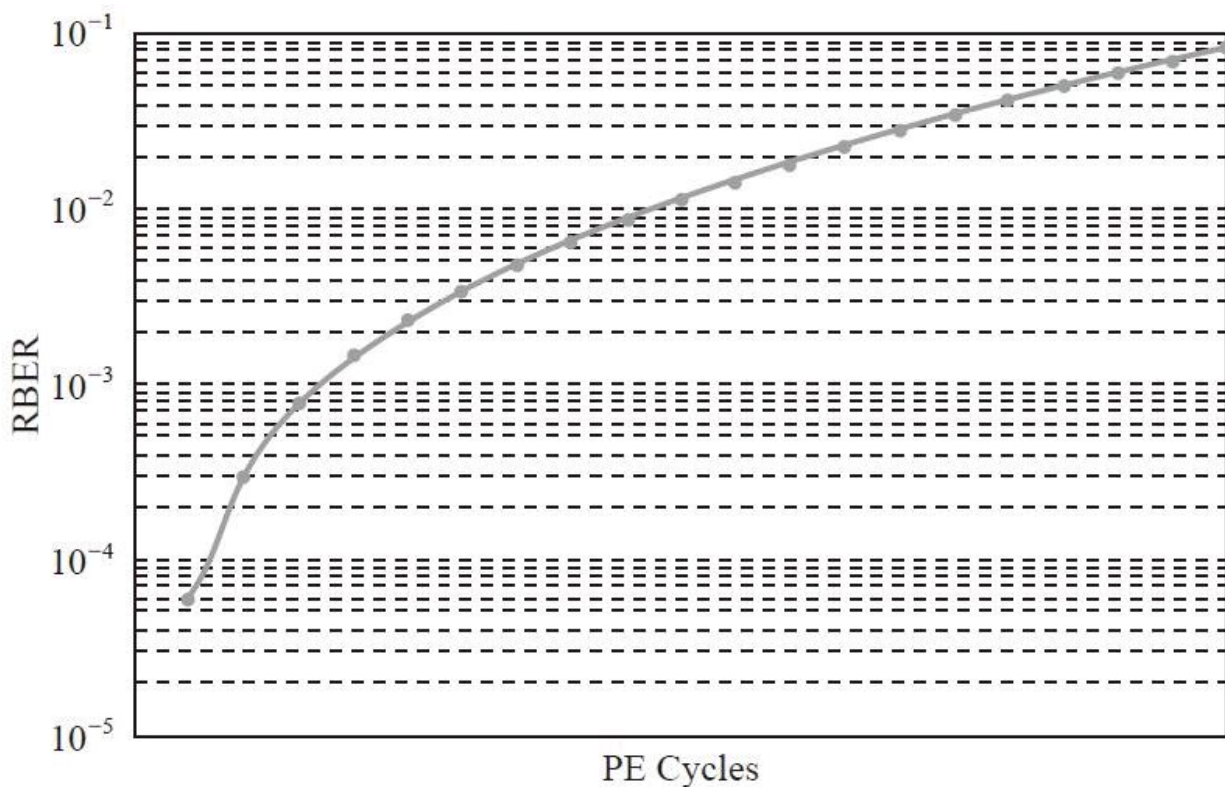


图1-26 RBER和PE的关系

RBER还跟闪存内部结构也有关系。两个相邻闪存块的RBER有可能完全不同，图1-27是单个闪存块里面不同闪存页的RBER分布图。看

得出来，Upper Page的RBER比Lower Page的RBER要高两个数量级。

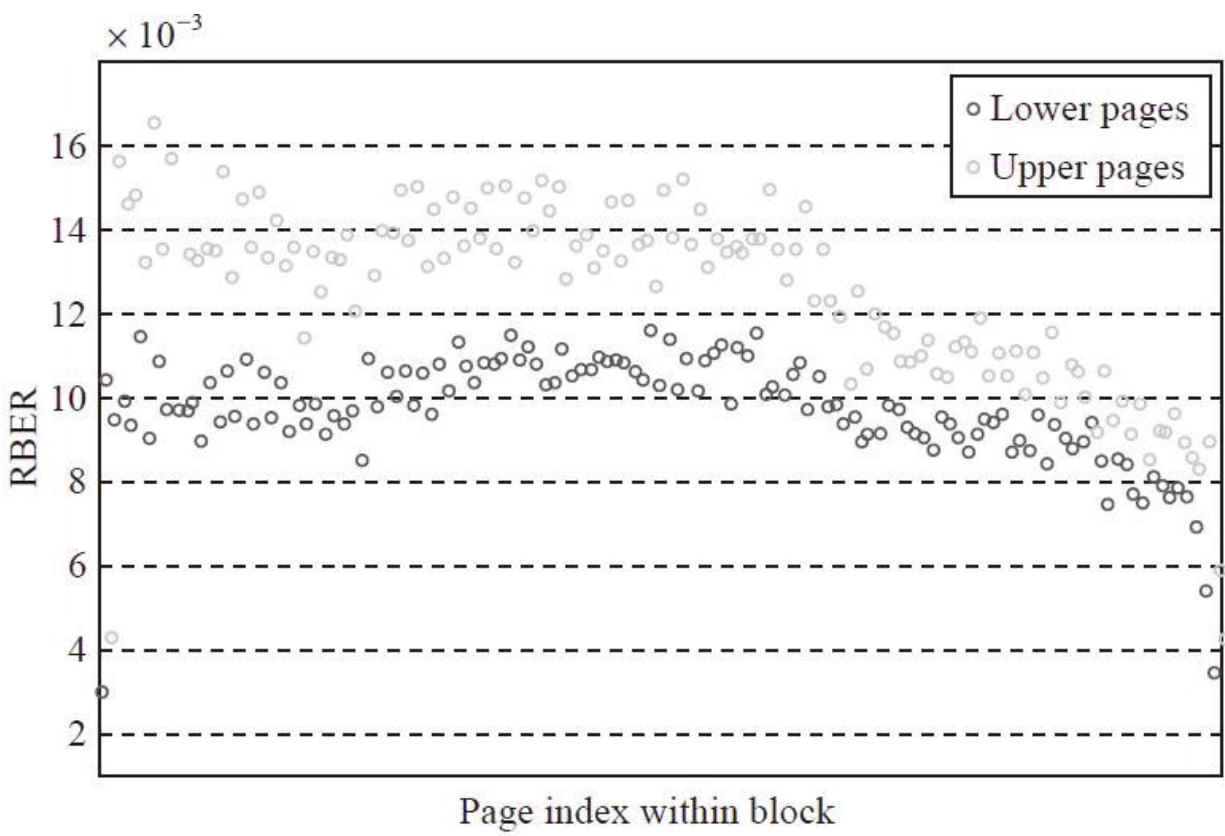


图1-27 Lower&Upper page RBER

通常商用企业级和消费级SSD的UBER指标如表1-9所示。

表1-9 企业级和消费级SSD的UBER值需求

	UBER
企业级 (Enterprise)	10^{-17} 甚至 10^{-18}
消费级 (Client)	10^{-15}

2.MTBF

工业界MTBF指标反映的是产品的无故障连续运行时间，也是产品的可靠性指标。MTBF计算有一些标准，目前最通用的权威性标准是MIL-HDBK-217、GJB/Z299B和Bellcore，分别用于军工产品和民用产

品。其中，MIL-HDBK-217是由美国国防部可靠性分析中心及Rome实验室提出的，现已成为行业标准，专门用于军工产品MTBF值的计算；GJB/Z299B是我国的军用标准；Bellcore是由AT&T贝尔实验室提出的，现已成为商用电子产品MTBF值计算的行业标准。

MTBF主要考虑的是产品中每个器件的失效率。但由于器件在不同的环境、不同的使用条件下其失效率会有很大的区别，例如，同一产品在不同的环境下，如在实验室和海洋平台上，其可靠性值肯定是不一样的；又如一个额定电压为16V的电容在实际电压为25V和5V下的条件失效率肯定也是不同的。所以，在计算可靠性指标时，必须考虑多种因素。所有这些因素几乎无法通过人工进行计算，但借助软件（如MTBFcal软件）和其庞大的参数库，能够轻松得出MTBF值。

对于SSD而言，JESD218A标准定义了测试SSD每天读/写量的方法，还补充了SSD一些额外的失败测试。要考虑的另一件事是：什么工作负载用于测试MTBF？例如合格的SSD使用工作负载每天写20GB，一共5年，基于这个工作负载加上补充性失效测试，这款SSD MTBF可达到120万小时。但如果工作量减少到每天写10GB，MTBF将变为250万小时；如果每天写5GB，就是400万小时。

1.5.5 功耗和其他剖析

1.SSD产品功耗

SSD定义了以下几种功耗类型：

·空闲（Idle）功耗：当主机无任何命令发给SSD，SSD处于空闲状态但也没有进入省电模式时，设备所消耗的功耗。

·Max active功耗：最大功耗是SSD处于最大工作负载下所消耗的功耗，SSD的最大工作负载条件一般是连续写，让闪存并发忙写和主控ASIC满负荷工作，这时的功耗值对应最大功耗。

·Standby/Sleep功耗：规范规定了SSD状态，包括：Active、Idle、Standby和Sleep，功耗值从Active到Sleep逐级递减，具体的实现由各商家自行定义。一般来讲，在Standby和Sleep状态下，设备应尽可能把不工作的硬件模块关闭，降低功耗。一般消费级SSD Standby和Sleep功耗为100~500mW。

·DevSleep功耗：这是SATA和PCIe新定义的一种功耗标准，目的是在Standby和Sleep基础上再降一级功耗，配合主机和操作系统完成系统在休眠状态下（如Hibernate），SSD关掉一切自身模块，处于极致低功耗模式，甚至是零功耗。一般是10mW以下。

对于主机而言，它的功耗状态和SSD作为设备端是一一对应的，而功耗模式发起端是主机，SSD被动执行和切换对应功耗状态。

系统Power State（SATA SSD作为OS盘）：

·S0：工作模式，OS可以管理SATA SSD的Power State，D0或者D3都可以。

·S1：是低唤醒延迟的状态，系统上下文不会丢失（CPU和Chipset），硬件负责维持所有的系统上下文。

·S2：与S1相似，不同的是处理器和系统Cache上下文会丢失（OS负责维护Cache和处理器上下文）。收到唤醒要求后，从处理器的reset

vector开始执行。

·S3: 睡眠模式（Sleep），CPU不运行指令，SATA SSD关闭，除了内存之外的所有上下文都会丢失。硬件会保存一部分处理器和L2cache配置上下文，从处理器的reset vector开始执行。

·S4: 休眠模式（Hibernation），CPU不运行指令，SATA SSD关闭，DDR内容写入SSD中，所有的系统上下文都会丢失，OS负责上下文的保存与恢复。

·S5: Soft off state，与S4相似，但OS不会保存和恢复系统上下文。消耗很少的电能，可通过鼠标键盘等设备唤醒。

进入功耗模式有一定的时延，当然退出功耗模式也需要一定的时延，通常恢复SSD到初始功耗模式所花费的时间更长，如表1-10所示。

表1-10 各种功耗模式下SSD进入和退出的时间

SSD 链路状态	功耗 (mW)	进入 (s)	退出 (s)	SSD 链路状态	功耗 (mW)	进入 (s)	退出 (s)
Active (Ready)	> 1000	0	0	Idle (DEVSLP)	5	0.02	0.02
Idle (Partial)	100	10^{-6}	10^{-4}	Off-RTD3	0	1.5	0.5
Idle (Slumber)	50	10^{-3}	0.01				

时延和性能之间存在着某种平衡，频繁的低功耗模式和正常模式之间换入换出，一定会带来性能的损失。对于SSD设备功耗模块设计而言，建议：尽可能优化低功耗模式的进入和退出时间。

从正常工作模式Active状态切换到低功耗模式，需要找到正确的切换Timer。太短的Timer会较早进入低功耗模式，但唤醒需要时延，带来主机端性能损失；太长的Timer有利于维持性能，但牺牲了功耗。

总之低功耗是一个好的SSD特性，消费级出于低功耗需求，极其需要这个特性，但企业级应用为了维持性能，在低功耗上是弱需求。

最后，SSD各项功耗是SSD产品的竞争力，尤其是对功耗敏感的消费级SSD的部署，最大写入功耗和低功耗是竞争力。最大写入功耗代表的是写入同样数据量所消耗的电能，主要是闪存写入功耗；低功耗是当用户空闲或休眠时设备节省下来的电能，这些对绿色能源数据中心

等场合有很大帮助。我们来看看几款消费级SSD功耗的对比，如图1-28所示。

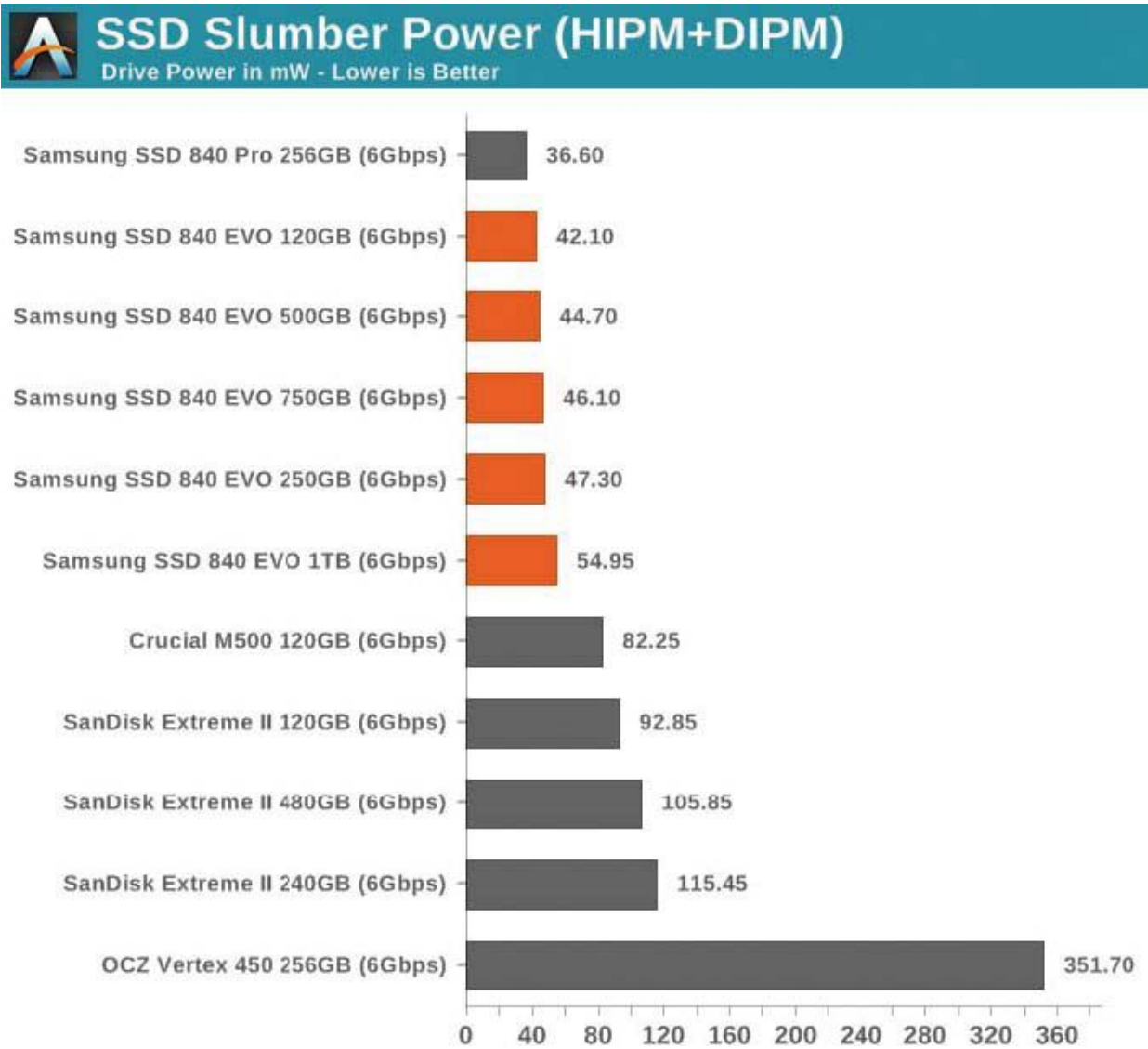


图1-28 AnandTech对几款SATA SSD的HIPM或DIPM slumber模式的低功耗对比

最大写入功耗对比（除了ASIC主控和板级PCB工作状态功耗，最大写入功耗和连续写性能紧密相关，写性能越高，功耗越高）如图1-29所示。

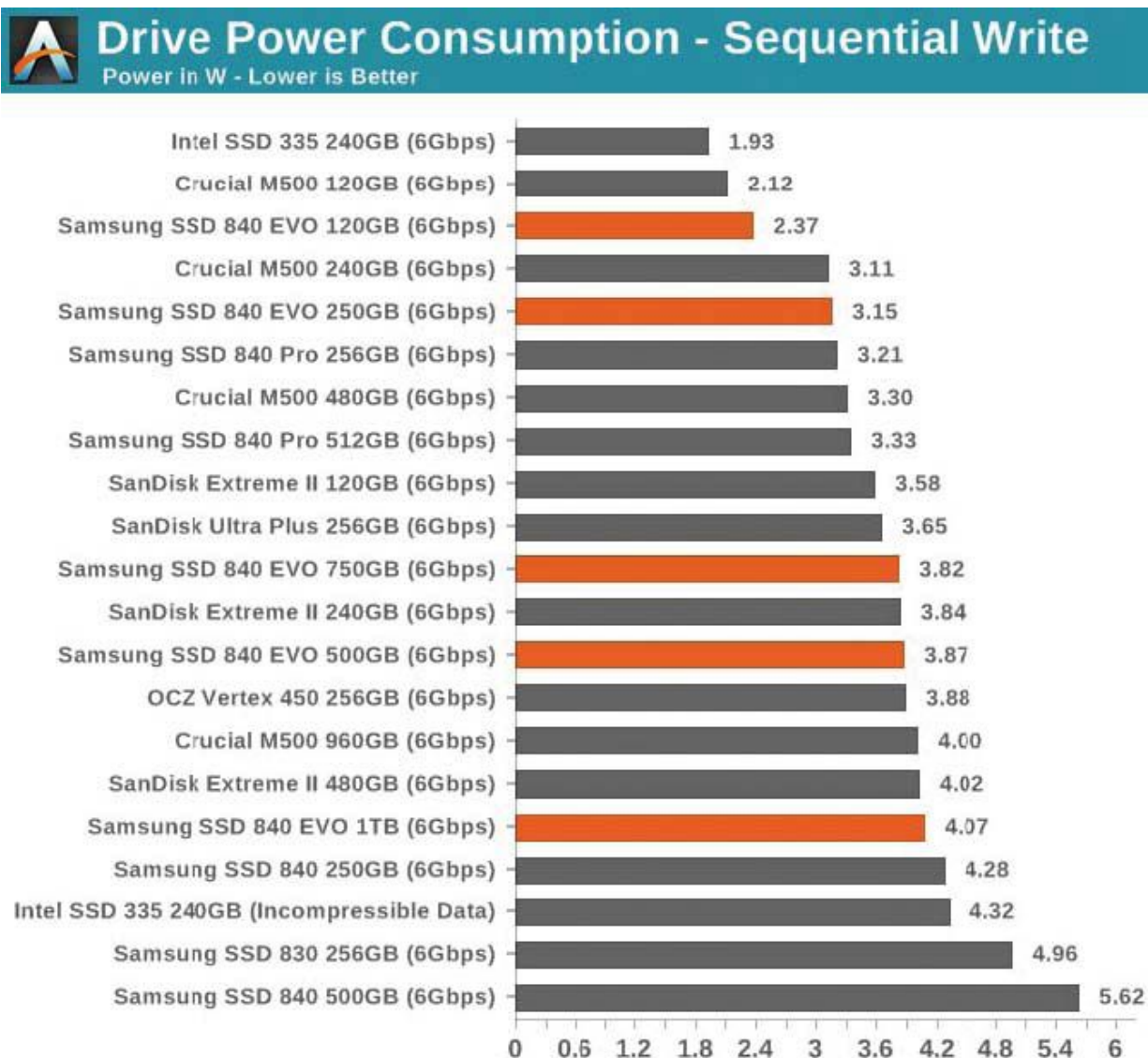


图1-29 AnandTech对比几款SSD的最大写入功耗

2.最大工作功耗与发热控制

前面已解释过最大工作功耗，单独把最大工作功耗拉出来讨论，是因为当SSD一直处于最大功耗工作负载下，器件会存在发热问题。为SSD功耗最大的是ASIC主控和闪存模块，因此二者也是发热大户，当热量积累到一定程度，器件会损坏掉，这是一定不能容忍的。当外界环境温度（Ambient Temperature）处在50℃或60℃时，不加以控制，发热的速度和损坏器件的概率也会随之增大。所以工作在最大负载下，控制SSD温度是固件设计要考虑的，就是设计降温处理算法。

做法具体的原理：当SSD温度传感器侦测到温度达到阈值，如70℃，固件启动降温算法模块，限制闪存后端并发写的个数，由于SSD中发热大户是闪存芯片，故当写并发数减少后，温度自然下降。同时由于写并发下降，SSD写性能也会下降，这是性能和温度的一个折中。

当温度控制下降到低于阈值70℃后，SSD固件重新恢复到正常的后端写并发个数，性能又会上升，带来温度再次上升，如此往复.....如图1-30所示。

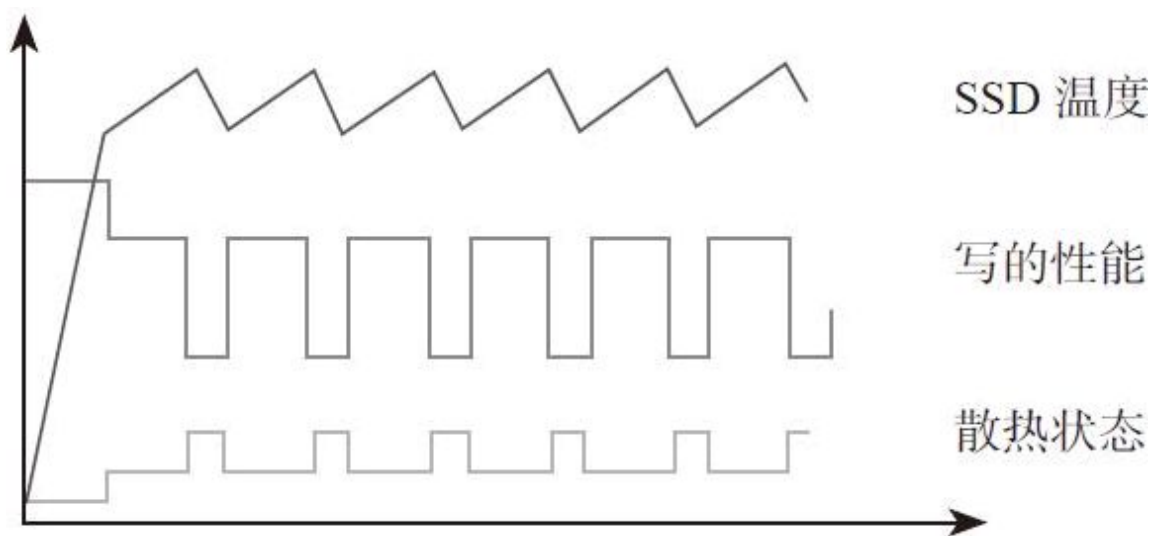


图1-30 温度控制和SSD性能的关系

1.5.6 SSD系统兼容性

SSD的各项参数中，系统兼容性指标无法量化，最不直观，也最容易被忽视。但不可否认的是，实际应用场合中除了性能功耗和可靠性问题，最让人头疼的是系统兼容性问题，表现为各种场景下盘无法识别、不兼容某些型号主板、操作系统无法兼容等问题。站在用户角度，SSD盘的性能、功耗、可靠性设计得都不错，测试出来的成绩单很漂亮，但就是系统兼容性差，再好的盘放到电脑上就变砖，看上去就是漂亮的花瓶，中看不中用。所以渐渐地用户开始重视系统兼容性问题，在SSD引入前期用比较强的测试覆盖去验证和观察系统兼容性。

从技术上系统兼容性问题归类为如下几类。

1.BIOS和操作系统的兼容性

SSD上电加载后，主机BIOS开始自检，主机中的BIOS作为第一层软件和SSD进行交互：第一步，和SSD发生链接，SATA和PCIe走不同的底层链路链接，协商（negotiate）到正确的速度上（当然，不同接口也会有上下兼容的问题），自此主机端和SSD连接成功；第二步，发出识别盘的命令（如SATA Identify）来读取盘的基本信息，基本信息包括产品part number、FW版本号、产品版本号等，BIOS会验证信息的格式和数据的正确性，然后BIOS会走到第三步去读取盘其他信息，如SMART，直到BIOS找到硬盘上的主引导记录MBR，加载MBR；第四步，MBR开始读取硬盘分区表DPT，找到活动分区中的分区引导记录PBR，并且把控制权交给PBR.....最后，SSD通过数据读写功能来完成最后的OS加载。完成以上所有这些步骤就标志着BIOS和OS在SSD上电加载成功。任何一步发生错误，都会导致SSD交互失败，进而导致系统启动失败，弹出Error window或蓝屏。

对SSD而言，其功能已经通过了白盒黑盒测试，但上述的加载初始化流程以及特定的BIOS和OS版本结合的相关功能测试并没有覆盖到，所以涉及这些功能有时可能会导致SSD设备加载失败。

由于现实世界中有太多的主板型号和版本号，一块兼容性良好的SSD需要在这些主机上都能正常运行。从测试角度来看，系统兼容性

认证包括以下各个方面：

- OS种类（Windows、Linux）和各种版本的OS；
- 主板上CPU南北桥芯片组型号（Intel、AMD）和各个版本；
- BIOS的各个版本；
- 特殊应用程序类型和各个版本（性能BenchMark工具、Oracle数据库.....）。

2.电信号兼容性和硬件兼容性

电信号兼容性和硬件兼容性指的是SSD工作时，主机提供的电信号处于非稳定状态，比如存在抖动、信号完整性差等情况，但依然在规范误差范围内，此时SSD通过自身的硬件设计（比如power regulator）和接口信号完整性设计依然能正常工作，数据也依然能正确收发。同理，在低温、电磁干扰的环境下，SSD通过硬件设计要有足够的鲁棒性（Robust）。

3.容错处理

错误处理与硬件和软件相关。系统兼容性的容错特指在主机端发生错误的条件下，SSD盘即使不能正常和主机交互数据，至少不能变砖。当然，SSD盘若能容错并返回错误状态给主机，提供足够的日志来帮助主机软硬件开发人员调试就更好了。这里的错误包括接口总线上的数据CRC错误、丢包、数据命令格式错误、命令参数错误等。

从设计角度考虑加入容错模块设计、加大系统兼容性测试的覆盖面，这些都是提高SSD系统兼容性的手段和方法。但从过去的经验看，系统兼容性重在对主机系统的理解，这需要长期积累经验，该趟的雷总是要趟的，趟过后就变成经验了，这些不是书本上能直接学到的。

最后要强调的是，SSD的系统兼容性是SSD的核心竞争力之一，不可忽视。

1.6 接口形态

SSD接口形态和尺寸的英文是SSD Form Factor。由于SSD是标准件，故它必须符合一定的接口规范、尺寸和电气特性，这样在应用层面才易于统一和部署，所以厂商和标准组织制定了Form Factor规范，SSD厂商和系统提供商都应遵守。

不同应用场景下的SSD，其Form Factor尺寸也不一样，如图1-31所示。表1-11列出了当下SATA、PCIe、SAS接口和协议的SSD所使用的Form Factor。

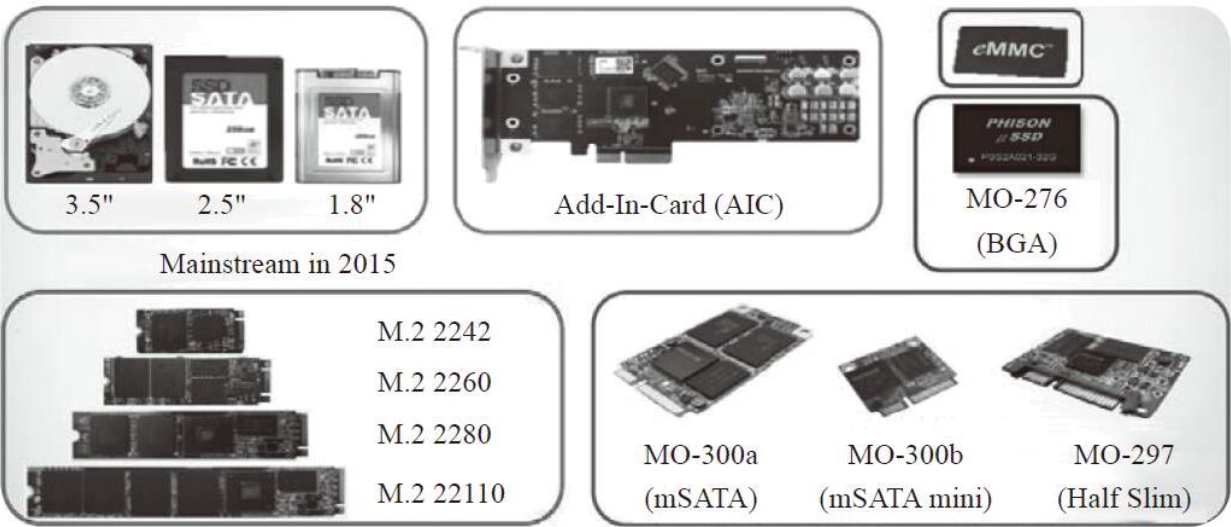


图1-31 各种类型的SSD示意图

表1-11 SSD form Factor和接口

	U.2	AIC	2.5"	Half slim	mSATA	M.2 22110	M.2 2280	M.2 2260	BGA uSSD
SATA	√		√	√	√	√	√	√	√
PCIe	√	√	√			√	√		√
SAS	√		√						

SATA SSD目前主要为消费级产品和企业级低端产品（如数据中心盘），这类产品接口和电气功能比较成熟，是目前出货量最大的SSD。它的Form Factor的种类比较多，其中消费级产品以M.2和2.5寸最为流行。消费级产品以SATA M.2为主导，企业级产品以SATA 2.5寸为主导。

PCIe SSD借助它的高性能、NVMe标准的制定和普及，以及软件生态的奠定，从2016年开始兴起。PCIe SSD Form Factor最开始起步于AIC（Add In Card），采用主板上插卡的形式，后演变到现在加入M.2和U.2形态。消费级PCIe SSD由M.2主导，企业级PCIe SSD多为2.5寸、U.2和AIC的形态。

SAS SSD基本上应用于企业级SSD，其借助成熟的SAS协议和软件生态，过去十年在企业级存储上大量应用。从HDD转换到SSD，虽然介质变了，但接口依然保留，原因是SAS在企业级应用已经普及，所以在传统的企业级存储阵列上，主要出货量还是SAS，形态为2.5寸。

mSATA是前些年出现的，与标准SATA相比体积大为缩小，主要用于消费级笔记本领域。但待M.2出现后，基本上替代了mSATA，革了它的命。

M.2原名是NGFF（Next Generation Form Factor），它是为超极本（Ultrabook）量身定做的新一代接口标准，主要用来取代mSATA接口，具备体积小巧、性能主流等特点。

U.2Form Factor（SFF-8639）起步于PCIe SSD 2.5寸盘形态制定的接口，到后来统一了SATA、SAS和PCIe三种物理接口，从而减小了下游SSD应用场合的接口复杂度，是一种新型连接器Form Factor，目前标准还在更新中。

1.6.1 2.5寸

2.5寸是主流企业级SSD的尺寸，这类SSD包括SATA、SAS和PCIe三种不同接口和性能的企业级SSD，1U存储和服务器的机架上可以放入20~30块硬盘，专为2.5寸尺寸设计。消费级SSD，尺寸主流包括2.5寸和更小尺寸的M.2，2.5寸多应用于桌面型PC，而轻薄型笔记本更多地使用M.2。

2.5寸也是HDD时代的笔记本硬盘的主流尺寸，到了后SSD时代，可以在笔记本和桌面型PC上沿用，但面对消费者更轻薄、更小硬盘的尺寸的需求，HDD就无能为力了，SSD依然可以往更小尺寸的方向发展。

对于2.5寸SSD而言，由于闪存密度的逐年增大，往这个盒子里塞入的容量可以越来越大，比如有了3层PCB的16TB、32TB容量的SSD，这是高密度SSD发展的一种趋势。

表1-12 SSD规格尺寸

尺寸（英寸）	三围			最大承载容量
	长（mm）	宽（mm）	高（mm）	
3.5	146	101.6	19, 25.4 or 26	12 TB HDD（2016 年）
2.5	100	69.85	5, 7, 9.5, 12.5, 15 or 19	32TB SSD（2017 年）

1.6.2 M.2

如图1-32所示，首先看看M.2 Form Factor（包括M.2普通和BGA SSD）的三围标准：Type 1216、Type 1620、Type 1630、Type 2024、Type 2226、Type 2228、Type 2230、Type 2242、Type 2260、Type 2280、Type 2828、Type 3026、Type 3030、Type 3042、Type 22110，前两个数字为宽度，后两个（或三个）数字是高度。注意，PM971就是Type 1620，厚度需要另外定义，单面贴片和双面贴片厚度大小不同。对于对厚度有要求的，比如平板电脑，一般采用单面贴片。

实际上四个（或五个）数字并不能完整定义M.2 SSD Form Factor，PCI-SIG定义了更完整的命名规则，包括宽、高、厚度信息和接口定义。如D2对应双面，单面厚度是1.35mm；B-M是M.2 connector key ID，表示同时支持PCIe x2、x4和SATA接口；等等。其他参数定义参考图1-33，图中明确定义了宽、高、厚尺寸和接口总线形式，甚至可以支持USB/SD卡接口，同时又保留了一些总线接口。总之M.2只是规范了一种引脚物理形式，它上面走什么协议和总线，要看具体的产品。

这里需要解释一下B和M key，这是两种主流的M.2 key定义，B也叫Socket2，M叫Socket3，B+M表示同时支持Socket2和Socket3。B和M的区别在于：M多了PCIe x4，可以支持4个通道，接口带宽最高可以到4GB/s，实际上Top和Bottom两面都有接口金手指，引脚数翻倍；B仅支持SATA/PCIe x2，接口带宽最高可以到2GB/s，仅支持Top面金手指引脚。M/Socket3无论在消费级还是企业级都是未来主流形式。

NOTE: KEY OPTION IS A REPRESENTATION ONLY
AND DOES NOT PROHIBIT ADDITION OPTIONS

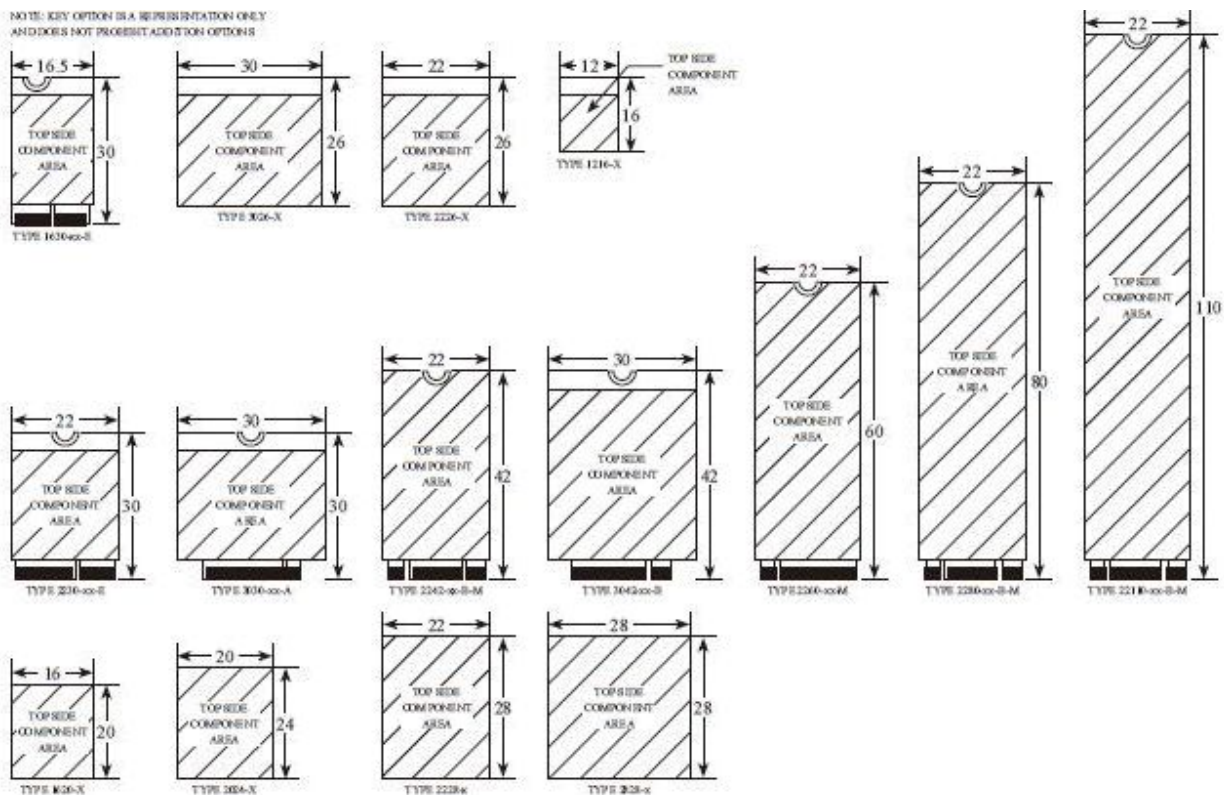


图1-32 各种不同M.2规格

Type XX XX-XX-X-X*			Key ID	Pin	Interface
Width (mm)	Length (mm)	Label**	Component Max Ht (mm)		
			Top Max	Bottom Max	
12	16	S1	1.2 ⁽¹⁾	0****	A 8-15 2 × PCIe × 1/USB 2.0/12C/DP × 4
16	20	S2	1.3 ⁽¹⁾	0****	B 12-19 PCIe × 2/SATA/USB 2.0/USB 3.0/HS IC/SIC/Audio/UIM/I2C
20	24	S3	1.5 ⁽¹⁾	0****	C 16-23 Reserved for Future Use
22	26	S4	1.7 ⁽¹⁾	0****	D 20-27 Reserved for Future Use
28	28	S5	2.0	0****	E 24-31 2 × PCIe × 1/USB 2.0/12C/SDIO/UART/PCM
30	30	D1	1.2	1.35	F 28-35 Future Memory Interface (FMI)
	42	D2	1.35	1.35	G 39-46 Generic (Not used for M.2)***
	60	D3	1.5	1.35	H 43-50 Reserved for Future Use
	80	D4	1.5	0.7	J 47-54 Reserved for Future Use
	110	D5	1.5	1.5	K 51-58 Reserved for Future Use
					L 55-62 Reserved for Future Use
					M 59-66 PCIe × 4/SATA

图1-33 M.2的命名规则

1.6.3 BGA SSD

1.BGA SSD的出现

半导体的发展规律是从单个分立元件到高度集成化。想象一下，过去的单个HDD，从只能存储几十MB的庞然大物发展到现在一个能装下几十TB的2.5寸SSD，这些都是半导体技术进步、制程进步和生产制造进步带来的。

SSD也走在这条规律的道路，随着制程和封装技术的成熟，当今一个PCB 2.5寸大小的存储器可以放到一个16mm×20mm BGA封装中，这就是BGA uSSD，如图1-34所示。

早在几年前，Intel和几家公司就在讨论在消费级平板或笔记本市场推出M.2BGA SSD及其标准，如比较传统的M.22260/2280/22110SSD，它有几点技术优势：

- 节省了15%以上的平台空间；
- 增加了10%的电池寿命；
- 节省了0.5mm～1.5mm SSD本身的高度；
- 具有更好的散热性（由于是BGA封装，热可以由ball pin传导到PCB板散出）。

实际上那时候标准规范滞后，SSD也才刚刚兴起，BGA封装技术还不成熟并且还缺乏消费级平台主板的支持，故并没有在消费级笔记本和平板上看到BGA M.2的产品，在工业级和其他小细分市场倒是有少量的BGA SSD在售。2016年PM971被三星投放到市场，从而拉开了BGA SSD在消费级平板类产品普及的大幕，预测各大厂商随后会推出相应的竞品，让我们拭目以待。当然了，在BGA SSD普及的过程中，关键还是要看价格，只要OEM价格到位，普及不是问题。

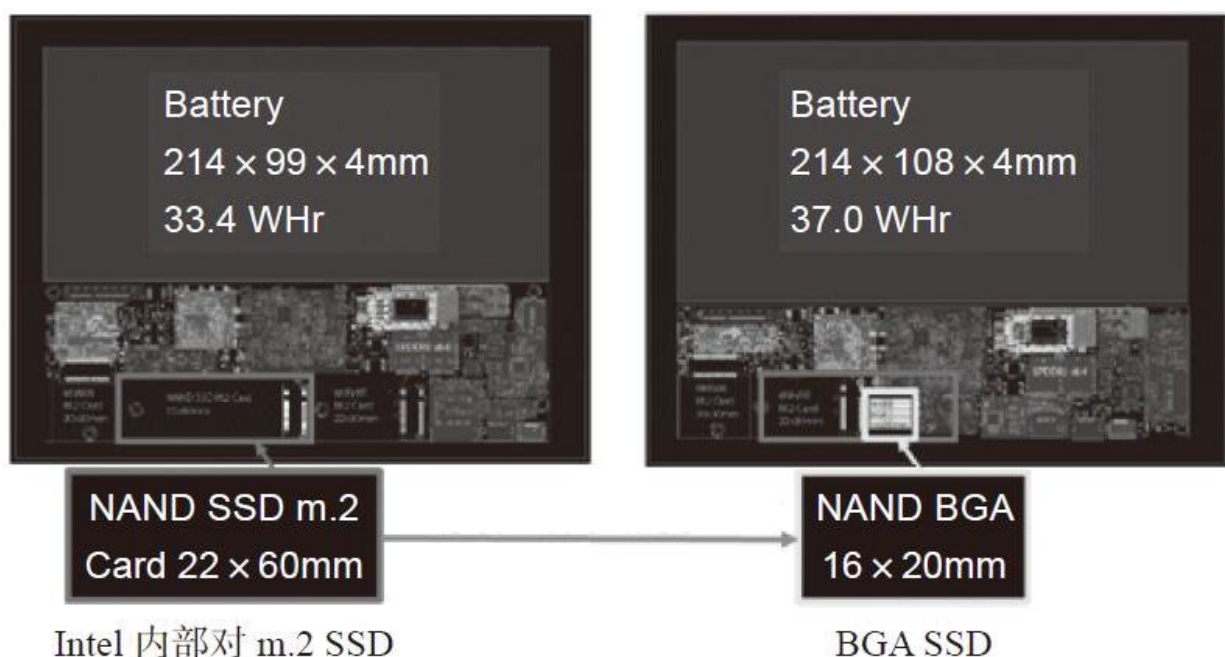


图1-34 传统M.2SSD与BGA SSD空间占用对比

BGA uSSD引脚纳入M.2标准，包括Type 1620、Type 2024、Type 2228、Type 2828，主流的是Type 1620。

2.江波龙P900PCIe BGA SSD

2017年7月14日，国内存储行业的领跑者深圳市江波龙电子有限公司（Longsys）率先发布目前世界上最小尺寸的NVMe PCIe SSD（11.5mm×13mm），主要是面向嵌入式存储应用，包括二合一电脑、超薄笔记本、VR虚拟现实、智能汽车等。新推出的FORESEEPCIe® BGA SSD，以P900命名，如图1-35所示。该产品在2017年8月8日硅谷的FMS（全球闪存峰会）2017及9月6日深圳洲际酒店CFM（中国闪存市场峰会）2017亮相。

2016年，Flash原厂相继发布了16mm×20mm的PCIe BGA SSD产品。而江波龙此次发布的P900系列，设计尺寸仅为11.5mm×13mm（见图1-36），是目前（2017年）世界上最小尺寸的SSD，其与手机中的eMMC及UFS的尺寸一样大小，但是容量要大得多。



图1-35 江波龙P900PCIe BGA SSD

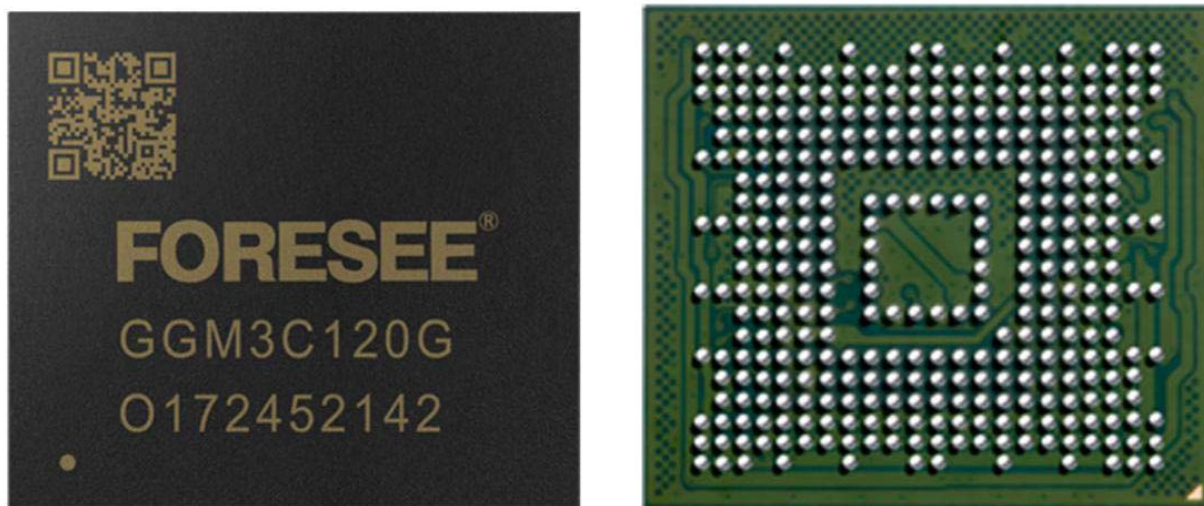


图1-36 江波龙Longsys新品: FORESEE® NVMe PCIe BGA SSD
(11.5mm*13mm)

而在容量方面，P900系列可提供512GB、256GB、128GB以及60GB等多种选择。江波龙计划在2017.Q4向客户提供样品，2018.Q1量

产，并面向全球销售。

P900支持PCIe Gen3.0x2接口与NVMe1.3协议，且主控配备带硬件加速器的嵌入式SRAM。江波龙自己开发固件用于优化IOPS性能，使用LDPC支持3D NAND Flash，可实现TLC存储器驱动器的高耐用性。

P900可以支持微软HMB（Host Memory Buffer）功能，有了这一功能，SSD不再需要额外搭配DRAM，只需要借助系统内存就能达到高性能的要求，同时成本和功耗更低。

另外，P900系列可以支持Boot Partition的功能，相当于把BIOS/UEFI系统整合到SSD里面。主机不再需要额外用SPI Flash作为系统引导，这样可降低这些设备的成本。

而在NAND Flash部分，P900采用最新制程的64层3D TLC，相比于2D TLC，64层3D TLC拥有更高的存储密度、更低的成本、更好的耐久性和更高的性能（见图1-37）。

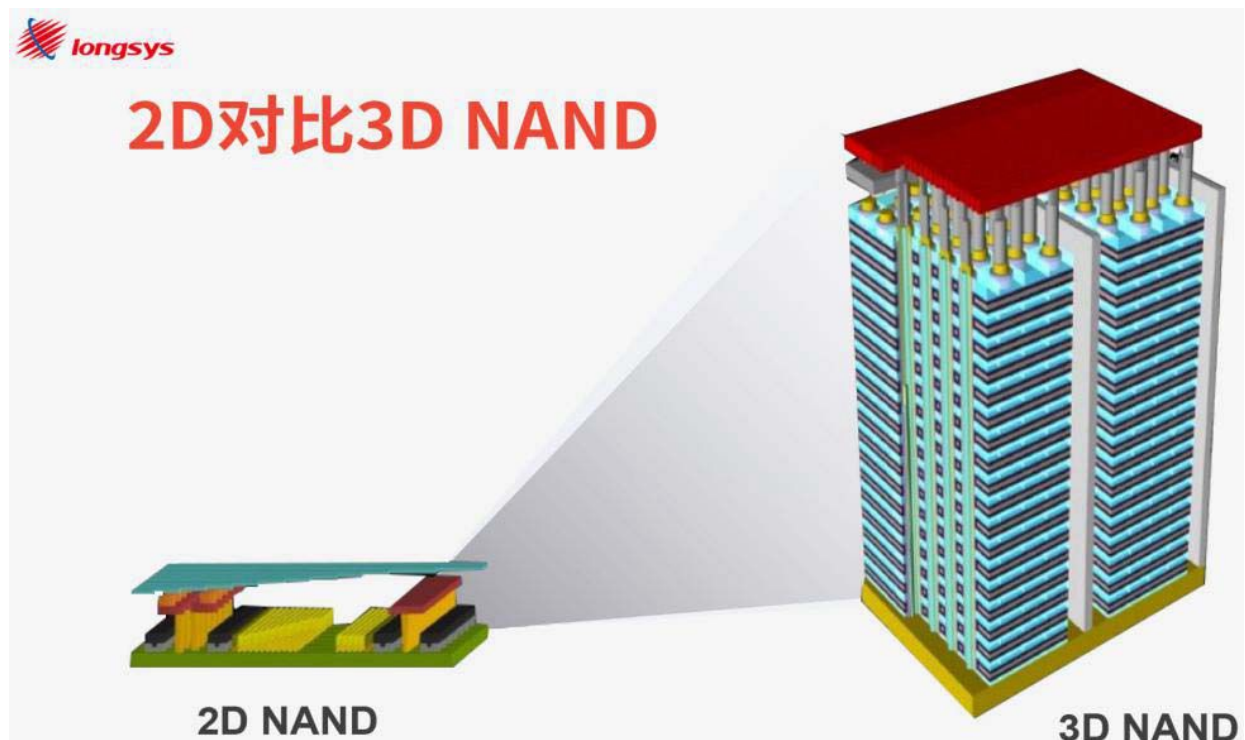


图1-37 2D和3D闪存对比

“将闪存应用到极致”是江波龙的工作目标。作为存储行业的创新者，江波龙基于3D NAND Flash会不断创新、厚积薄发。江波龙在存储

行业已耕耘了近20年，一直在努力开发新技术、新产品、新存储商业模式，这也体现了做中国存储的风格。

1.6.4 SDP

2016年8月25日，国内存储行业领军企业深圳市江波龙电子有限公司开创性地推出了SSD的一体化模块产品——SDP™（见图1-38），从而为消费类SSD的零售渠道市场及商业模式带来革命性的改变。

SDP™就是SATA Disk in Package，是指将SSD主控芯片、闪存芯片在封装厂封装成一体化模块，经过开卡量产、测试后出厂。这种产品形态相当于SSD的半成品，只需要加上外壳就能成为完整的SSD产品。SDP™具有尺寸小、功耗低、质量轻等亮点，其尺寸大小仅为33.4×17.2×1.23mm（见图1-39），功耗低至1430mW，质量仅为1.9g。

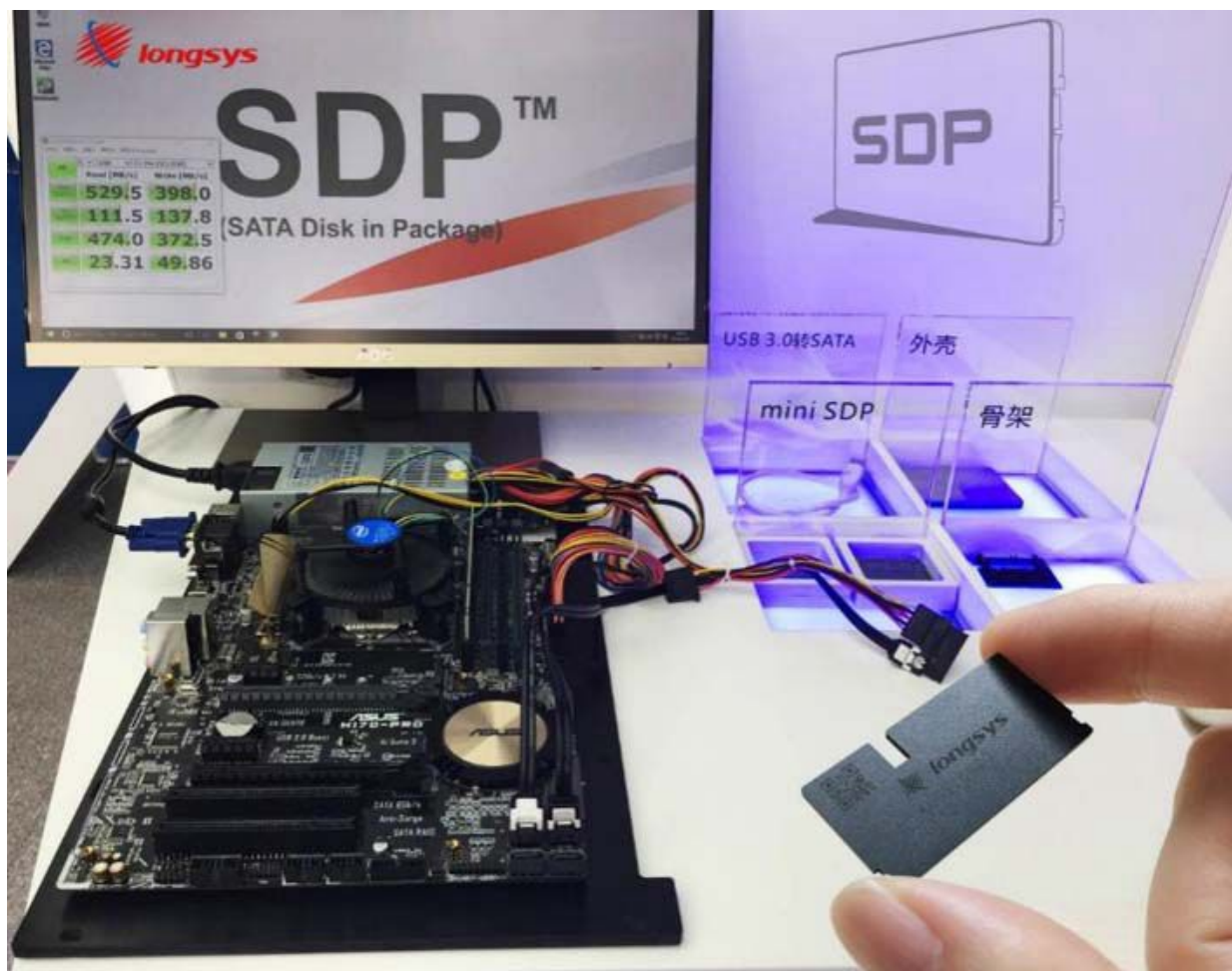


图1-38 江波龙展出SDPTM量产样品



图1-39 江波龙SDPTM产品与标准SD卡对比

与传统PCBA模式相比，SDP™ 具备哪些优势？具体如图1-40所示。

SDP™与PCBA的对比

类别 产品	品质	灵活度	CKD	库存管理
	高	好	非常适合	轻松
	中低	差	不适合	复杂难处理

图1-40 江波龙SDPTM与传统PCBA的对比

由于采用了模块化的制造方式，相对于传统的PCBA制造方式，SDP™ 产品可以将SSD成品生产时间从以前的15天缩短到1天。产能从15K/天扩大到100K/天，同时具有更稳定的品质以及更短的交货时间等优点。

1.6.5 U.2

U.2俗称SFF-8639，这是新生产物，采用非AIC形式，以盘的形态存在。开发U.2的目的是统一SAS、SATA、PCIe三种接口，方便用户部署。其标准至本书完稿时还在不断更新和补充中。不可否认的是，在PCIe取代SATA甚至SAS的未来，U.2连接器和Form Factor会成为企业级SSD盘存在的主要形态，PCIe接口成为主要接口。

1.7 固态存储市场

1.7.1 SSD正在取代HDD

从2000年年初SSD雏形诞生，到几大闪存原厂布局SSD产品，SSD经历了用户对闪存和数据可靠性的质疑，到实际产品的试水、铺开，一直到2015年才掀起SSD替换HDD的浪潮。到2017年，消费级SSD市场中SSD的装机率已到30%~40%，预测在2018年，SSD装机率将超过50%，如图1-41所示。



图1-41 SSD装机率

市场的数据一方面表达SSD的普及率，更重要的是表达了未来SSD的成长性。不可否认的是，SSD已经有主导存储设备市场的趋势，完全或大部分替代HDD成为主流存储器只是时间问题。所以对于希捷和西数HDD厂商而言，HDD销量下滑、拥抱SSD是可以预见的必然趋势。

在性能、可靠性、功耗等方面完爆HDD的SSD，未来装机率和普及率（Market Share）的快慢主要取决于SSD的价格，更核心的是闪存单位GB价格的变化，图1-42所示是SSD与HDD相比价格的趋势预测。

至本书截稿时，128GB SSD的价格和1TB HDD的价格基本相当，但每GB的SSD与HDD相比仍然有8倍的差距。按照摩尔定律推算，闪存密度在快速增大，这给每GB闪存的价格下降提供了绝佳的通道，SSD价格和成本问题得到解决后，其前途一片光明。

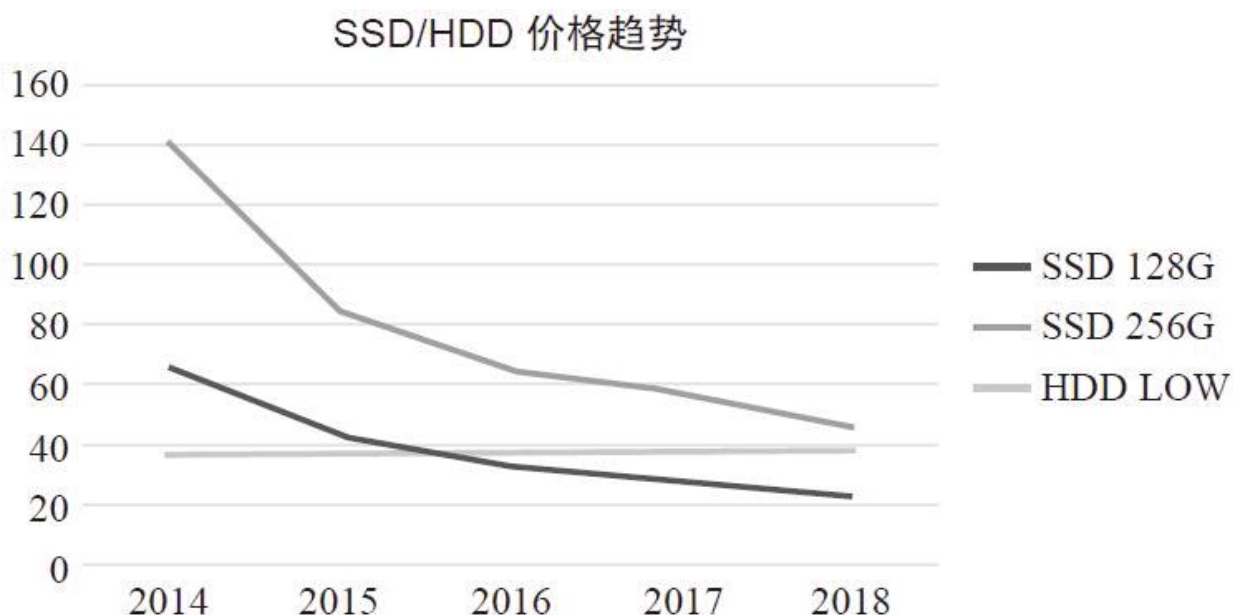


图1-42 SSD与HDD的价格对比

1.7.2 SSD、HDD应用场合

数据按照热度的不同会采取不同的存储方式，这样可以平衡性能和成本的问题，俗称性价比。在HDD和SSD二分天下的今天，SSD主要用于存放和用户贴近的热数据，其对总容量需求较小，性能优先；HDD主要用于存放和用户较远的温（warm）数据或冷（cold）数据，其对总容量需求较大，价格优先。这是一种设计的平衡。具体来讲：

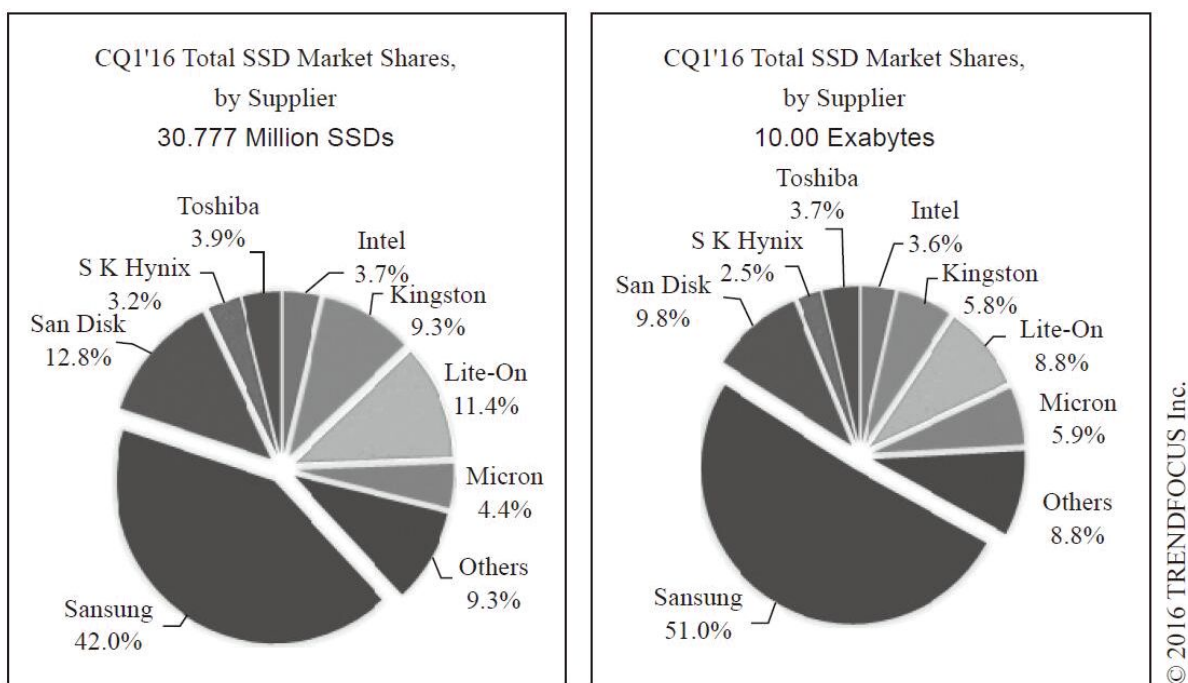
- 数据加速层：采用PCIe接口的高性能的SSD。
- 热数据（频繁访问）层：采用普通SATA、SAS SSD。
- 温数据层：采用高性能HDD。
- 冷数据层：采用HDD。
- 归档层：采用大容量价格低廉的HDD，甚至磁带。

1.7.3 SSD市场情况

从2016年Trend Focus的SSD市场占有率调研来看，总体来说三星（Samsung）领跑整个市场，占据SSD市场的半壁江山如图1-43所示。三星在主控、介质技术和市场方面占有主导优势，尤其是其介质，领先竞争对手1~2年的优势。在可预见的未来，闪存原厂会主导SSD市场，尤其是成本和售价竞争激烈的消费级SSD市场。原因是SSD 90%以上的成本取决于闪存，闪存厂商对闪存的成本和供应有自主权。

当然，非闪存原厂在SSD领域也有不少成功的玩家，像Lite-ON、Kingston，凭借过往在闪存、内存模组产品的销售渠道，切入消费级SSD市场，占据5%~10%的市场份额，在SSD成长过程中分得一杯羹。

SSD的研发模式，三方配合：主控厂商+闪存厂商+生产制造。对于闪存大厂而言，有自己的主控和闪存颗粒，研发的核心部分掌握在自己手中。对于没有主控和闪存颗粒的SSD厂商而言，凭借品牌和渠道优势，通过引入第三方主控厂商（包括Turnkey FW）和自己购买闪存，若成本控制得当，SSD的生产和销售体系也能建立起来，做得比较成功的有Lite-ON、Kingston。总之SSD的市场是闪存原厂、主控厂商、SSD渠道销售商三方共舞的市场。



TRENDFOCUS

The Data Storage Industry's Most Trusted Market Intelligence

图1-43 2016各家SSD厂商市占率

第2章 SSD主控和全闪存阵列

如前所述，SSD主要由两大模块构成——主控和闪存介质。其实除了上述两大模块外，可选的还有缓存单元。主控是SSD的大脑，承担着指挥、运算和协调的作用，具体表现在：一是实现标准主机接口与主机通信；二是实现与闪存的通信；三是运行SSD内部FTL算法。可以说，一款主控芯片的好坏直接决定了SSD的性能、寿命和可靠性。本章将聚焦SSD主控。

2.1 SSD系统架构

SSD作为数据存储设备，其实是一种典型的（System on Chip）单机系统，有主控CPU、RAM、操作加速器、总线、数据编码译码等模块（见图2-1），操作对象为协议、数据命令、介质，操作目的是写入和读取用户数据。

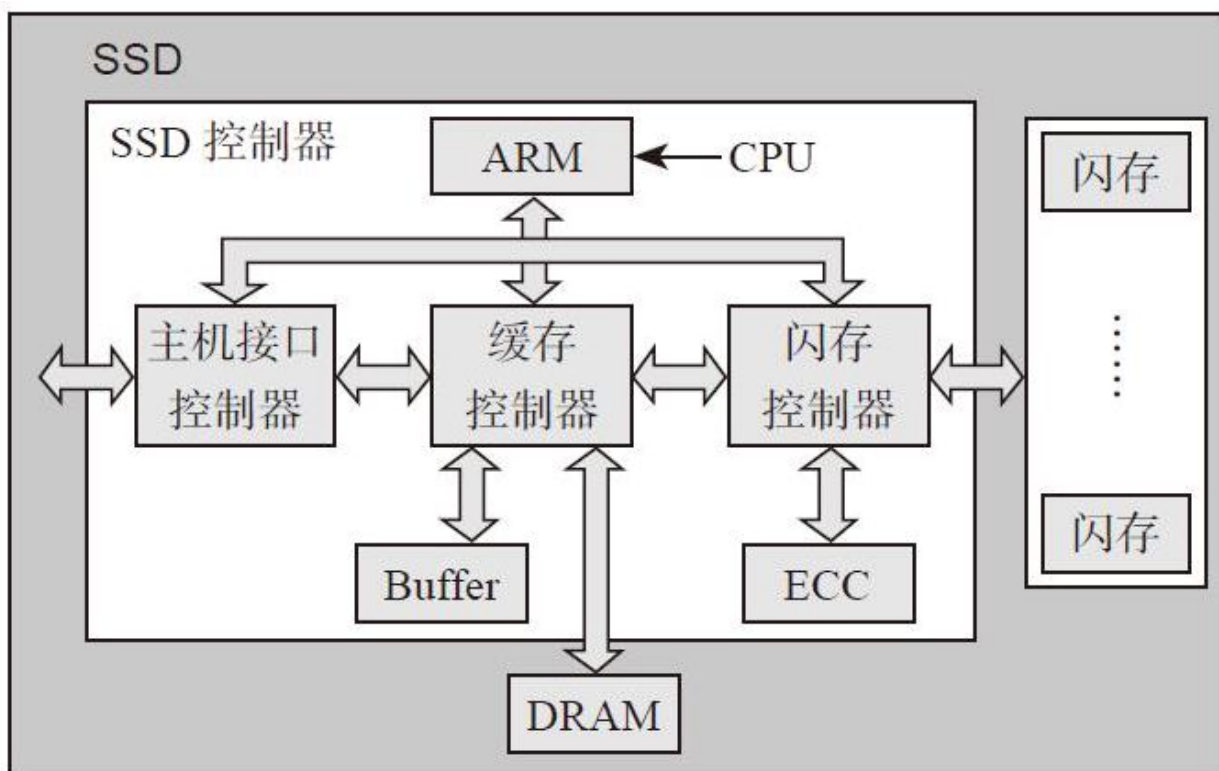


图2-1 SSD主控模块硬件图

图2-1所示仅是一个SSD系统架构的概略图，这款主控采用ARM CPU，主要分为前端和后端两大部分。前端（Host Interface Controller，主机接口控制器）跟主机打交道，接口可以是SATA、PCIe、SAS等。后端（Flash Controller，闪存控制器）跟闪存打交道并完成数据编解码和ECC。除此之外还有缓冲（Buffer）、DRAM。模块之间通过AXI高速和APB低速总线互联互通，完成信息和数据的通信。在此基础上，由SSD固件开发者构筑固件（Firmware）统一完成SSD产品所需要的功能，调度各个硬件模块，完成数据从主机端到闪存端的写入和读取。

2.1.1 前端

主机接口：与主机进行通信（数据交互）的标准协议接口，当前主要代表为SATA、SAS和PCIe等。表2-1所示是三者的接口速率。

表2-1 SATA、SAS、PCIe接口速率

接口	速率（Gbps）
SATA	6/3/1.5
SAS	12/6
PCIe	通道数 × 8（PCIe3.0）

SATA的全称是Serial Advanced Technology Attachment（串行高级技术附件），是一种基于行业标准的串行硬件驱动器接口，是由Intel、IBM、Dell、APT、Maxtor和Seagate公司共同提出的硬盘接口规范（见图2-2）。2001年，由Intel、APT、Dell、IBM、希捷、迈拓这几大厂商组成的SATA委员会正式确立了SATA 1.0规范。

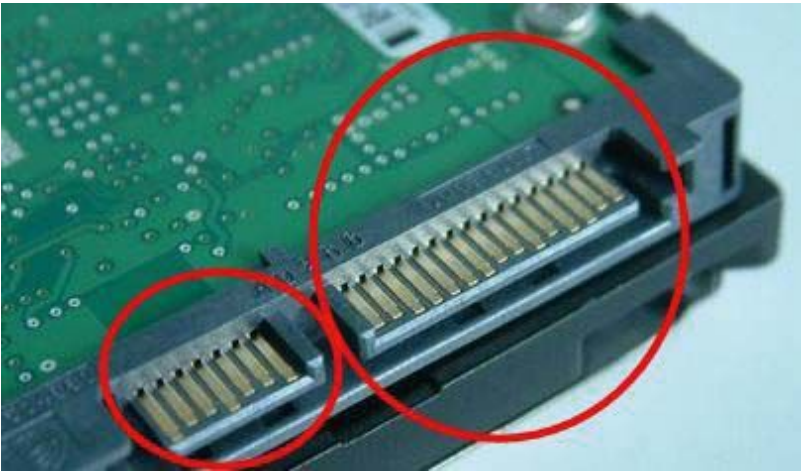


图2-2 SATA接口

SAS（Serial Attached SCSI）即串行连接SCSI，是新一代的SCSI技术，和现在流行的Serial ATA（SATA）硬盘相同，都是采用串行技术以

获得更高的传输速度，并通过缩短连接线改善内部空间等（见图2-3）。SAS是并行SCSI接口之后开发出的全新接口，此接口的设计是为了改善存储系统的效能、可用性和扩充性，并且提供与SATA硬盘的兼容性。SAS的接口技术可以向下兼容SATA。具体来说，二者的兼容性主要体现在物理层和协议层。在物理层，SAS接口和SATA接口完全兼容，SATA硬盘可以直接用在SAS的环境中；从接口标准上而言，SATA是SAS的一个子标准，因此SAS控制器可以直接操控SATA硬盘，但是SAS却不能直接用在SATA的环境中，因为SATA控制器并不能对SAS硬盘进行控制。在协议层，SAS由3种类型的协议组成，根据连接设备的不同使用相应的协议进行数据传输。其中串行SCSI协议（SSP）用于传输SCSI命令；SCSI管理协议（SMP）用于对连接设备的维护和管理；SATA通道协议（STP）用于SAS和SATA之间数据的传输。因此在这3种协议的配合下，SAS可以和SATA以及部分SCSI设备无缝结合。



图2-3 SAS接口

PCIe（Peripheral Component Interconnect Express）是一种高速串行计算机扩展总线标准，它原来的名称为3GIO，是由英特尔在2001年提出的，旨在替代旧的PCI、PCI-X和AGP总线标准。PCIe属于高速串行点对点多通道高带宽传输，所连接的设备分配独享通道带宽，不共享总线带宽，主要支持主动电源管理、错误报告、端对端的可靠性传

输、热插拔以及服务质量（QoS，Quality of Service）等功能。它的主要优势就是数据传输速率高，目前最高的4.0版本可达到2GB/s（单向单通道速率），而且还有相当大的发展潜力。PCI Express也有多种规格，从PCI Express 1X到PCI Express 32X，意思就是1个通道到32个通道，能满足将来一段时间内出现的低速设备和高速设备的需求。PCI-Express最新的接口是PCIe 4.0接口。

图2-4和图2-5展示的是PCIe接口，分别为卡式和U.2。

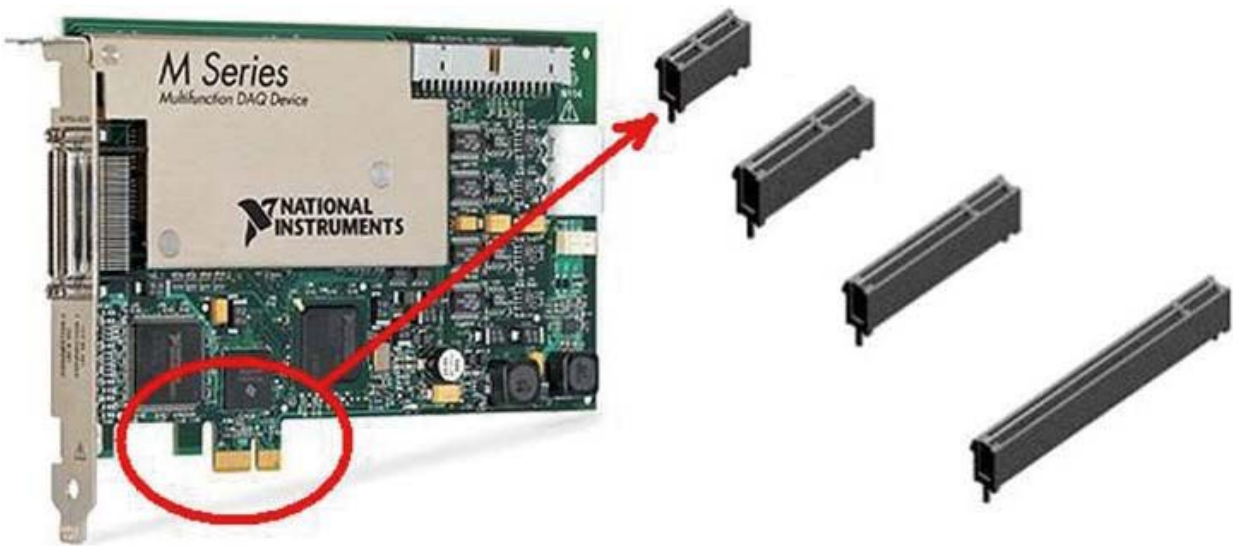


图2-4 PCIe接口式插卡（AIC）



图2-5 U.2接口

前端是负责主机和SSD设备通信的接口，命令和数据传输通过前端总线流向或流出SSD设备。

从硬件模块上来看，前端有SATA/SAS/PCIe PHY层，俗称物理层，接收串行比特数据流，转化成数字信号给前端后续模块处理。这些模块处理NVMe/SATA/SAS命令，它们接收并处理一条条命令和数据信息，涉及数据搬移会使用到DMA。一般命令信息会排队放到队列中，数据会放到SRAM快速介质中。如果涉及加密和压缩功能，前端会有相应的硬件模块来做处理，若软件无法应对压缩和加密的快速需求，则会成为性能的瓶颈。

从协议角度，以一条SATA Write FPDMA命令为例对上述内容进行说明。从主机端文件系统发出一条写命令请求，该请求到主板南桥AHCI寄存器后，AHCI寄存器执行请求，即进行写操作，忽略文件系统到AHCI路径的操作细节，从SSD前端总线上看会发出如下的写交互操作（见图2-6）：

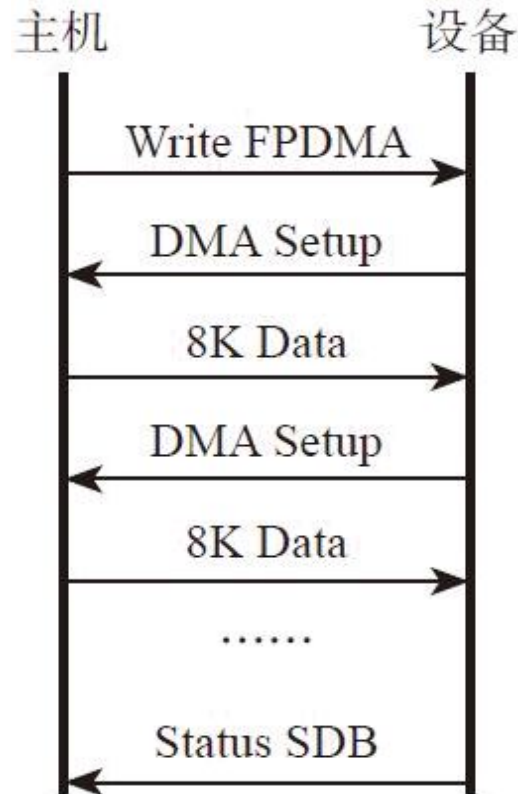


图2-6 SAT A Write FPDMA命令协议处理步骤

步骤1：主机在总线上发出Write FPDMA命令FIS（Frame Information Structure，帧信息结构，是SATA为了实现异步传输数据块而使用的封包）。

步骤2：SSD收到命令后，判断自己内部写缓存（Write Buffer）是否有空间去接收新的数据。如果有，则发出DMA Setup FIS到主机端；否则什么也不发，主机端处于等待状态（这叫流控：数据流量控制）。

步骤3：主机端收到DMA Setup FIS后，发送不大于8KB数据的Data FIS给设备。

步骤4：重复步骤2和步骤3直到数据全部发送完毕。

步骤5：设备（SSD）发送一个状态Status FIS给主机，表示从协议层面这条写命令完成全部操作。当然Status可以是一个good status或者一个bad/error status，表示这条Write FPDMA命令操作正常或者异常完成。

SSD接收命令和数据并放到SSD内部缓冲区之后还需要做些什么呢？任务还没完成，前端固件模块还需要对命令进行解析，并分派任务给中端FTL。命令解析（**Command Decoder**）将命令FIS解析成固件和FTL（**Flash Translation Layer**）能理解的元素：

- 这是一条什么命令，命令属性是读还是写（注意，本处是写命令）；

- 这条写命令的起始LBA和数据长度；

- 这条写命令的其他属性，如是否是FUA命令，和前一条命令LBA是否连续（是连续命令还是随机命令）。

当命令解析完成后，放入命令队列里等待中端FTL排队去处理。由于已经有了起始LBA和数据长度两大主要信息元素，FTL可以准确地映射LBA空间到闪存的物理空间。至此，前端硬件和固件模块完成了它应该完成的任务。

2.1.2 主控CPU

SSD控制器SoC模块和其他嵌入式系统SoC模块并没有什么本质的不同，一般由一颗或多颗CPU核组成，同时片上有I-RAM、D-RAM、PLL、IO、UART、高低速总线等外围电路模块。CPU负责运算、系统调度，IO完成必要的输入输出，总线连接前后端模块。

通常我们所说的固件就运行在CPU核上，分别有代码存储区I-RAM和数据存储区D-RAM。如果是多核CPU，需要注意的是软件可以是对称多处理（SMP）和非对称多处理（AMP）。对称多处理多核共享OS和同一份执行代码，非对称多处理是多核分别执行不同代码。前者多核共享一份I-RAM和D-RAM，资源共享；后者每核对应一份I-RAM和D-RAM，每核独立运行，没有内存抢占导致代码速度执行变慢的问题。当SSD的CPU要求计算能力更高时，除增加核数和单核CPU频率外，AMP的设计方式更加适应计算和任务独立的要求，消除了代码和数据资源抢占导致执行速度过慢的问题。

固件根据CPU的核数进行设计，充分发挥多核CPU的计算能力是固件设计考虑的一方面。另外，固件会考虑任务划分，会将任务分别加载到不同CPU上执行，在达到并行处理的同时让所有CPU有着合理且均衡的负载，不至于有的CPU忙死有的CPU闲死，这是固件架构设计要考虑的重要内容，目标是让SSD输出最大的读写性能。

SSD的CPU外围模块包括UART、GPIO、JTAG，这些都是程序必不可少的调试端口，另外还有定时器模块Timer及其他内部模块，比如DMA、温度传感器、Power regulator模块等。

2.1.3 后端

本节将从SSD主控角度来分析一下后端硬件模块。

后端两大模块分别为ECC模块和闪存控制器（见图2-7）。

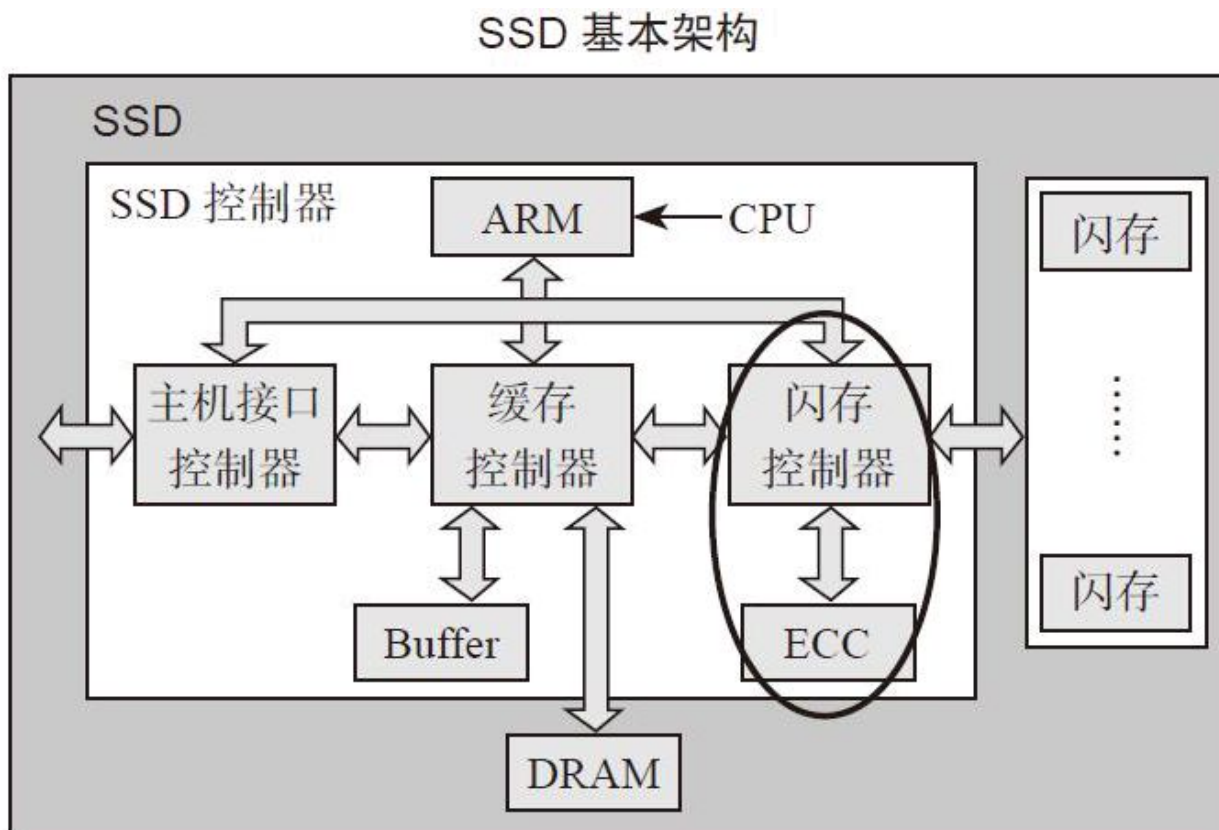


图2-7 SSD中的ECC模块和闪存控制器

ECC模块是数据编解码单元，由于闪存存储天生存在误码率，为了数据的正确性，在数据写入操作时应给原数据加入ECC校验保护，这是一个编码过程。读取数据时，同样需要通过解码来检错和纠错，如果错误的比特数超过ECC纠错能力，数据会以“不可纠错”的形式上传给主机。这里的ECC编码和解码的过程就是由ECC模块单元来完成的。SSD内的ECC算法主要有BCH和LDPC，其中LDPC正逐渐成为主流。

闪存控制器使用符合闪存ONFI、Toggle标准的闪存命令，负责管理数据从缓存到闪存的读取和写入。

闪存控制器如何和闪存连接和通信？从单个闪存角度看，一个Die/LUN是一个闪存命令执行的基本单元，闪存控制器和闪存连接引脚按照如下操作（见图2-8）：

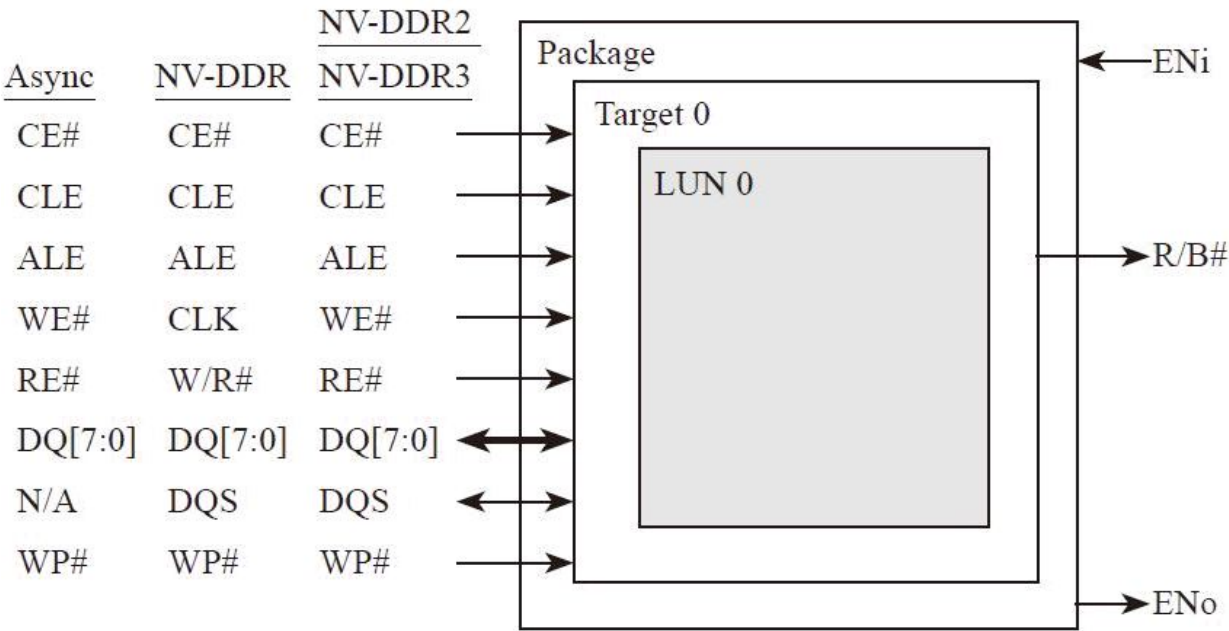


图2-8 闪存芯片接口

·外部接口：8个IO接口，5个使能信号（ALE、CLE、WE#、RE#、CE#），1个状态引脚（R/B#），1个写保护引脚（WP#）；

·命令、地址、数据都通过8个IO接口输入输出；

·写入命令、地址、数据时，都需要将WE#、CE#信号同时拉低，数据在WE#上升沿被锁存；

·CLE、ALE用来区分IO引脚上传输的是数据还是地址。

从闪存控制器角度看，为了性能需求需要并发多个闪存Die/LUN，通常配置有多个通道（channel）。一个通道挂多少个闪存Die/LUN，取决于SSD容量和性能需求，Die/LUN个数越多，并发的个数越多，性能越好。

Die/LUN是闪存通信的最小基本管理单元，配有上述的一套总线，即8个I/O口，5个使能信号（ALE、CLE、WE#、RE#、CE#），1个状态引脚（R/B#），1个写保护引脚（WP#）.....

如果一个通道上挂了多个闪存Die/LUN，每个Die共用每个通道上的一套总线，那闪存控制器如何识别和哪个Die通信呢？答案是通过选通信号CE#实现。在闪存控制器给特定地址的闪存Die发读写命令和数据前，先选通对应Die的CE#信号，然后进行读写命令和数据的发送。一个通道上可以有多个CE，SSD主控一般设计为4~8个，对于容量而言选择有一定的灵活度。

2.2 SSD主控厂商

SSD主控是一个技术深度和市场广度都很大的芯片产品。SSD发展初期主控芯片玩家较少，原因是设计和生产一款新的芯片的要求和门槛较高。如今由于SSD的蓬勃发展，配套的主控厂商看到了发展前景和利润空间，纷纷切入这个产品，SSD主控初创公司如雨后春笋般出现。

下面介绍一下Marvell主控、三星主控和国内主控的技术深度和特色。

2.2.1 Marvell主控

Marvell是全球排名第一的HDD和SSD主控芯片供应商。2007年开始在SSD控制器领域进行布局，于2008年推出第一代SATA SSD产品Davinci。作为SSD主控领域的老大，Marvell的SSD产品线非常完善，覆盖了高中低端市场，产品形态上包括了SOC、ASIC及CSSP，如图2-9所示。

Marvell目前的主力产品包括主攻PC市场的SATA系列Dean（88SS1074），主攻PC、数据中心、云端市场的PCIe系列Eldora（88SS1093/88SS1092），还有针对入门级零售市场、享有创新DRAMless设计的Artemis系列（88NV1120/88NV1160）。

Marvell公司现在拥有超过1400项存储专利（还有大约200项专利正在申请）的强大知识产权组合。凭借在HDD领域二十多年的产品经验，Marvell在低功耗、高性能设计、封装、先进制程方面有了很多的积累。Marvell的主控技术均领先竞争对手两到三代（见图2-10）。无论是2D/3D MLC还是2D/3D TLC，也无论是SATA还是PCIe接口形式，Marvell都颇有建树。且Marvell与客户的关系好，合作伙伴包括金士顿、LiteOn、Micron、Toshiba、Seagate、Sandisk、江波龙、联想等国际国内大厂，持续引领着行业技术的变革与创新。

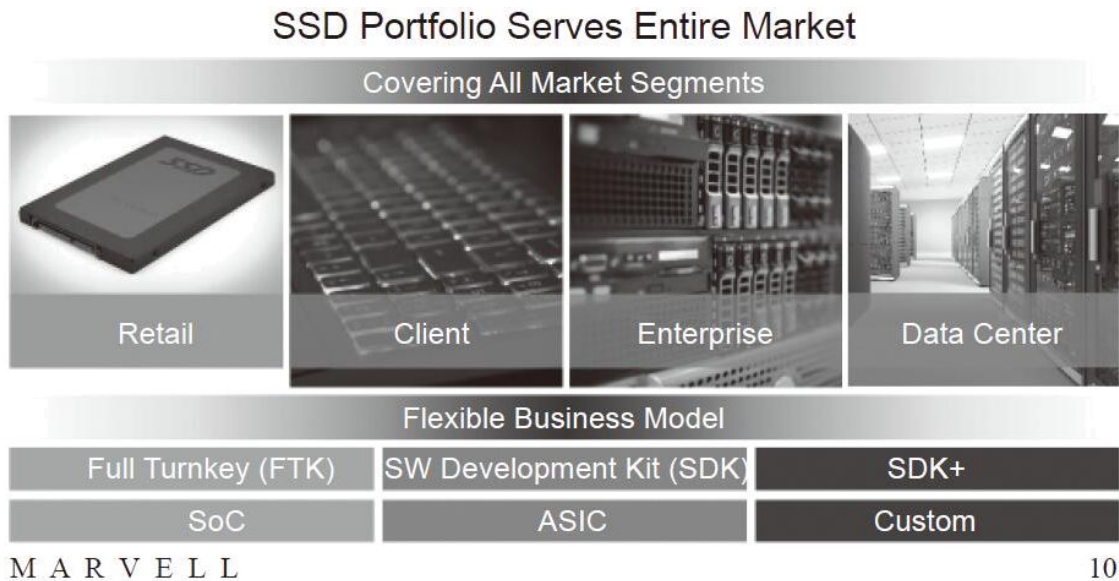


图2-9 Marvell SSD产品线覆盖零售、客户端、企业级及数据中心市场










Marvell SSD Technology Evolution	1 st Gen PCIe 	2 nd Gen PCIe 	3 rd Gen PCIe 	4 th Gen PCIe 	
	2010-2011 Plato	2012-2013 Brighton	2013-2014 Alta+	2015-2016 Eldora	
	<ul style="list-style-type: none">• Single Dragonite• PCIe Gen2 × 1 (5Gbps)• AHCI• 4CH × 4CE• ONFI2.2/Toggle1 @200 MB/s• Strong BCH• 65nm• 12 × 12mm package	<ul style="list-style-type: none">• Dual Dragonite @ 400Mhz• PCIe Gen2 × 2 (10Gbps)• AHCI• 8CH × 4CE• ONFI 3.0/Toggle2@400 MB/s• Strong BCH• 55nm• 17 × 17mm package	<ul style="list-style-type: none">• Dual Cortex R4 @ 400Mhz• PCIe Gen2 × 4 (20Gbps)• AHCI• 8CH × 4CE• ONFI 3.0/Toggle2@400 MB/s• BCH 2 level ECC• 40nm LPM• 17 × 17mm package	<ul style="list-style-type: none">• Triple Cortex R5 @ 500 Mhz• PCIe Gen3 × 4 (40Gbps)• AHCI/NVMe• 8CH × 8CE• ONFI 3.2/Toggle2 @ 533MB/s• LDPC Gen3• 28nm HPM• 17 × 17mm package	
	1 st Gen SATA 	2 nd Gen SATA 	3 rd Gen SATA 	4 th Gen SATA 	5 th Gen SATA 
	2008 Davinci	2009-2010 Van Gogh	2011-2012 Monet	2013-2014 Renoir	2015-2016 Dean
	<ul style="list-style-type: none">• Dual Dragonite @ 200Mhz• SATA II 3Gb/s• 8CH × 4CE• ONFI 2.0/Toggle1 @ 100MB/s• BCH15• 90nm• 17 × 17mm package	<ul style="list-style-type: none">• Dual Dragonite @ 250Mhz• SATA III 6Gb/s• 8CH × 4CE• ONFI 2.1/Toggle1 @ 133 MB/s• Strong BCH• 65nm• 17 × 17mm package	<ul style="list-style-type: none">• Dual Dragonite @ 400Mhz• SATA III 6Gb/s• 8CH × 4CE• ONFI 2.2/Toggle1 @ 166 MB/s• BCH2 level ECC• 55nm• 17 × 17mm package	<ul style="list-style-type: none">• Dual Dragonite @ 400 Mhz• SATA III 6Gb/s• 8CH × 4CE• ONFI 3.0/Toggle2 @ 400 MB/s• BCH2 level ECC• 55nm• 17 × 17mm package	<ul style="list-style-type: none">• Dual Dragonite @ 400 Mhz• SATA III 6Gb/s• 4CH × 8CE• ONFI 3.2/Toggle2 @ 533MB/s• LDPC Gen3• 28nm LP• 11 × 13.5mm package

图2-10 Marvell已推出五代SATA SSD产品以及第四代PCIe SSD主控产品

Marvell在高端SoC设计上处于领先地位，Marvell通过复杂的SoC架构、领先的纠错机制、接口技术、低功耗等多项优势建立起领先竞争对手的技术壁垒：

1) **Marvell专有的NANDEdge技术**。这种LDPC（低密度奇偶校验）纠错机制是目前业界任何其他功能所无法比拟的技术，Marvell公司所有最新的SATA、SAS和NVMe的SSD控制器都采用了该技术。NANDEdge技术适用于传统平面型和新兴3D堆叠三阶存储单元（TLC），以及四阶存储单元（QLC）NAND SSD，能够确保实现最高的耐用性、可靠性和数据完整性，并延长SSD的使用寿命。目前Marvell的LDPC校验技术已经迭代到了第三代。

2) 可扩展、可延续的开发架构。Marvell Artemis系列主控，是全球第一个支持PCIe NVMe的不需要DRAM缓存的SSD主控方案，并支持Host Memory Buffer (HMB) 特性。

3) 特性丰富的SDK。Marvell为合作伙伴提供了完善的SDK开发工具，不仅能加快上市时间，还能让合作伙伴有条件、有精力将自己的软件团队用于开发能体现差异化或自身优势的方面，从而实现差异化竞争。

4) 全产品线转向16nm工艺。Marvell在业界率先使用28nm工艺，而其他不少友商还停留在40nm甚至55nm。未来Marvell全产品线将转向16nm工艺，产品的尺寸会更小，功耗也将更低。



图2-11 Marvell将HDD领域技术优势延伸至SSD控制器产品中

无论在口碑上还是销量上，Marvell主控一直是市场的佼佼者。其中，88SS1074SATA SSD控制器在短短18个月内的出货量已超过5000万，年同比增长385%。Artemis系列产品88NV1140在CES 2016国际消费电子展上亦获得了Visions award。而最新的88NV1160DRAM-less SSD控制器则在美国ACE 2017逻辑/接口/存储器产品类别评选中摘得大奖。

2.2.2 三星主控

三星的主控基本上都是三星自己的SSD在用，830系列使用是MCX主控，而840及840Pro使用的则是MDX主控，850Pro/840EVO用的是MEX主控，850EVO 500GB以下的和750EVO用的是MGX主控，650用的是MFX主控，如图2-12所示。



图2-12 三星主控芯片

MCX是200MHz的三核ARM 9核心，缓存容量256MB；MDX的核心则换成300MHz的三核Cortex-R4处理器，缓存容量512MB；MEX则是把频率提升至400MHz，并且加入了TurboWrite技术的支持，缓存容量1GB。至于MGX和MFX主控，目前可以知道的是MGX是一个双核主控，而且三星优化了低容量下的随机性能；而MFX可能是一颗4通道主控。

2.2.3 国产主控，谁主沉浮

常见的台系主控包括智微（JMicron）、慧荣（Silicon Motion）和群联（Phison）三家公司的主控。它们成本低廉，相当受SSD厂家欢迎，现在有相当多的SSD在用这三家的主控。不过近年来，JMicron的产品已经渐渐淡出市场了，这里着重介绍慧荣和群联两家的主控。

1. 慧荣主控

慧荣科技（SMI）为全球闪存控制芯片及专业射频IC的市场先驱及技术领导者，慧荣从2000年开始提供记忆卡用的闪存控制芯片，一路走来，从CF、SD、USB，到进入手机用的嵌入式内存芯片eMMC/UFS及固态硬盘主控芯片，在每个领域都可说是闪存主控芯片的龙头厂商，至今已经出货超过50亿颗闪存控制芯片及超过1亿颗SSD固态硬盘主控芯片。

SMI长期与全球主要闪存大厂合作，无论是Samsung、Toshiba、WD/Sandisk、SKhynix、Micron还是Intel，SMI都为其提供了全面性主控芯片解决方案。借由与闪存大厂的合作关系，SMI可以在更早期以主控厂商的身份提供、回馈给闪存厂商技术方案，可以提前了解NAND的发展趋势，从而及早设计对应的主控及固件。近年来，英特尔消费性SSD也开始全面使用SMI的主控芯片，这证明SMI的SSD主控芯片质量是世界一流水平的。近期Crucial所发表的MX500即是采用SMI的SM2258H主控芯片，其上搭配了Micron 64层的TLC，证明SMI这几年SSD的领先技术已经获得国际大厂与消费者的认同。

慧荣提供一系列固态硬盘主控芯片（见图2-13），支持所有主要闪存大厂的MLC、TLC及SLC闪存，其应用范畴囊括个人计算机、消费性电子品、工业计算机与其他相关应用；同时支持最先进的安全协议；支持AES 128/256、TCG Opal Full-Drive等加密机制。

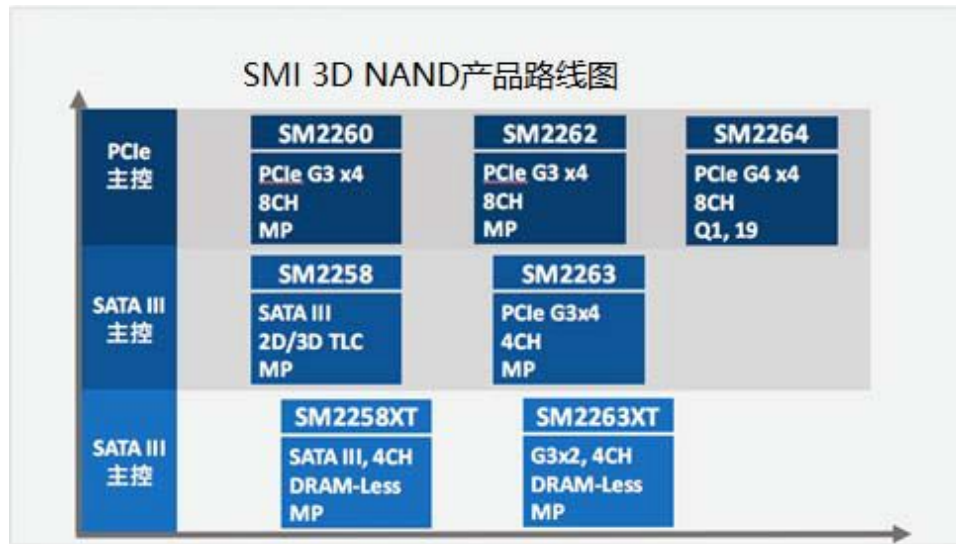


图2-13 SMI主要SSD控制器产品

SMI凭借着多年来开发闪存相关主控技术的积累，在SSD主控上面发展出几项竞争优势：

·客制化的交匙（Turnkey）方案：SMI在固态硬盘主控芯片上的主要优势在于，能够提供从主控芯片到固件方案，再到电路板设计、闪存颗粒的配对等一整套固态硬盘的解决方案，还能够根据采购厂商的个性化需求进行定制化的服务。慧荣提供的一站式服务，能够充分发挥主控芯片与固件方案紧密结合的优势，实现最大效能与最小功耗。

·NANDExtend专家ECC纠错方案：NANDExtend是SMI结合LDPC及多项SMI专利的纠错技术，可延长闪存使用寿命高达3倍。NANDExtend可以应用于MLC、TLC及QLC等不同存闪。SMI从2009年就开始致力于LDPC纠错技术，并且多次在国际会议上发布相关技术，目前已开发至第四代的LDPC纠错技术。

·自制的物理层（Physical layer, PHY）接口技术：SATA与PCIe SSD都需要用物理层来传输数据，有了自制的PHY，才能快速跟未来新的接口接轨并使用更新的半导体制程技术。从产品路线图上来看，SMI在2018年发表的PCIe Gen3x4 SSD主控上面已经全面转向28nm，PCIe Gen 4更会使用12nm，是目前能看到的第一个会使用12nm的SSD主控厂商。

慧荣虽然在SSD起步比其他主控公司来得晚，但凭借过去多年在各类闪存主控上的技术开发积累，这三年来在SSD方面飞快成长，一站式的方案更帮助了国内外许多自有品牌SSD制造商快速向终端市场推出极具技术竞争力的产品。除了原本的SATA SSD主控外，2017年更一次推出三颗第二代PCIe Gen3x4的主控芯片。2017年在深圳举行的闪存市场高峰会上，SMI也表示除了消费性SSD以外，他们也即将进军企业级的SSD主控以及软件定义存储（Software Defined Storage）的市场，持续扩大他们在固态存储方面的影响力。

2.群联主控

群联电子于2000年11月成立。从提供全球首颗单芯片U盘控制芯片起家，群联目前已经成为U盘、SD存储卡、eMMC、UFS、PATA与SATA固态硬盘等控制芯片领域的领头者。群联是ONFI（Open NAND Flash Interface）的创始人之一，同时也是SD协会的董事。群联主控如表2-2所示。

表2-2 群联主控列表

控制器型号	接口	DRAM	最大支持容量	通道	AES 支持	特色
PS3107-S7	SATAII	Optional	256GB	4	No	<ul style="list-style-type: none"> • BCH ECC • SmartRefresh TM • SmartFlush TM • GuaranteedFlush TM
PS3108-S8	SATAIII	DDR3	1TB	8	PS3108-A8	<ul style="list-style-type: none"> • BCH ECC • SmartRefresh TM • SmartFlush TM • GuaranteedFlush TM • 支持 DEVSLP
PS3109-S9	SATA III	LPSDR	256GB	4	PS3109-A9	<ul style="list-style-type: none"> • BCH ECC • SmartRefresh TM • SmartFlush TM • GuaranteedFlush TM • 支持 DEVSLP
PS3110-S10	SATA III	DDR3/DDR3L	2TB	8	PS3110-A10	<ul style="list-style-type: none"> • 端到端数据保护 • SmartECC TM • SmartRefresh TM • SmartFlush TM • GuaranteedFlush TM • 支持 DEVSLP • 支持 TLC Flash
PS3111-S11	SATA III	DRAM-less	1TB	2	No	<ul style="list-style-type: none"> • LDPC • 端到端数据保护 • SmartECC TM • SmartRefresh TM • SmartFlush TM • GuaranteedFlush TM • SmartZIP TM • 支持 DEVSLP • 支持 TLC • 支持 3D 闪存

(续)

控制器型号	接口	DRAM	最大支持容量	通道	AES 支持	特色
PS5007-E7	PCIe Gen3 × 4	DDR3L	2TB	8	PS5007-A7	<ul style="list-style-type: none"> • NVMe1.1b • PCIe3.0 • 端到端数据保护 • SmartECC™ • SmartRefresh™ • SmartFlush™ • GuaranteedFlush™ • 支持 TLC • 支持 L1.2 模式
PS5008-E8/E8T	PCIe Gen3 × 2	E8: DDR3&DDR3L E8T: DRAM-Less	E8: 2TB E8T: 1TB	4	YES	<ul style="list-style-type: none"> • NVMe1.2 • PCIExpress Rev.3.1 • 端到端数据保护 • StrongECC • SmartECC™ • SmartRefresh™ • SmartFlush™ • GuaranteedFlush™ • 支持 MLC/TLC/3D 闪存 • 支持 L1.2 模 • Single Root I/O • Virtualization • Pyrite

群联主控，因其中流的产品性能、低廉的价格以及全面的服务，和慧荣主控一样，深受中小厂商的追捧，也成为大牌厂商入门级产品的首选方案之一。

以上与控制器相关的信息来自群联官网：<http://www.phison.com>。

3.其他国产主控

固态硬盘市场近几年红得发紫，品牌商、代工厂、芯片设计公司各显神通，都期望在这个市场分一杯羹。那我们就来捋一捋国内其他地区自主SSD芯片设计公司，看谁有可能闯出一片天地。

海思毫无疑问是很强的，不过它的芯片只给华为用，所以就不列为讨论对象。剩下的就是记忆科技、湖南国科微、杭州华澜微；其他还有很多正在做的，但应该还没有做出正式芯片。

记忆靠着联想的关系，在内存市场做大，看到SSD在PC市场有前景，很早就切入到SSD领域。记忆理想远大，所以组建团队做SSD芯

片。切入的时间点很好，同时经过四五年的努力，已经出了一款SATA控制器，性能还不错，可靠性若可以再完善，那么就有希望把主控用自己的SSD上。拥有自己的主控后就具备了和其他主控讨价还价的能力，海思在早期就是华为用来和外资芯片议价的工具。

国科微在2016年1月发布了首款主控GK2101，其采用40nm工艺，支持SATA/NVMe/AHCI、8通道闪存和LDPC，这算是比较领先的了。尽管PCIe只有GEN2X4，不过相信他们下一代很快就会赶上。据说已经有客户开始测试，估计不久就可以实现量产。想当初，国科微在卫星芯片市场杀出重围，赚到第一桶金，在安防监控市场表现也不错，又有大基金加持，成功IPO上市。国科微通过第一代SSD主控在市场学到一些经验，若能把一些欠缺的技术补强，还是大有可为的。

华澜微最开始是做SD/MMC和U盘控制器的，在2016年年初收购了晶量半导体，所以也拥有了桥接芯片产品线。其在接口方面的竞争优势比较大，但目前看到的PCIe产品还是GEN2。可能是为了充分发挥自己桥接的优势，他们的主控和一般主控不同，采用类似桥接的方式，通过SATA转eMMC等来拼成一个SSD，这样主控就不需要FTL，开发难度会降低。不过鱼与熊掌不可兼得，拼接也有可能影响性能和寿命。但是也不是什么大问题，毕竟性能可通过上层算法优化，而且一般来讲，用户对性能要求并不是非常高；寿命可以通过RAID方式来补强，只要控制好整体成本就是好方案。

前面讲的都已经做出了产品的厂商，后面就讲讲正在做产品的厂商。虽说先发制人，但是芯片设计是马拉松竞赛，后发未必制于人，还有可能少走一些弯路。

2016年12月27日，北京得瑞领新科技有限公司（DERA）宣布推出自主研发的TAI控制器。支持NVMe 1.2标准及PCIe 3.0接口，4KB随机写IOPS可以达到500k，而4KB随机读更是可以达到1250k IOPS，顺序写读分别为4.5GB/s和5.1GB/s。目前已经成功流片，估计正在把产品弄稳定。DERA团队人数不多，但是不少核心成员来自最早做SSD的SST公司，有多年的SSD主控经历，所以能在这么短的时间内设计出一款高性能SSD主控。

忆芯（Starblaze）这个名字可能很多人不熟悉，但是说起Memblaze，大家就都知道了。忆芯团队核心成员来自Memblaze，2017

年年初独立为忆芯，第一颗测试芯片回来立马就完成了A轮，说明大家还是比较看好他们的前景的。

浪潮和山东华芯半导体专注安全固态硬盘，他们的SATA SSD控制器已经通过国家密码局芯片测试。研发团队由有硅谷背景的资深技术专家掌舵，相信会大有可为。

在安全存储领域，北京的中劼科技有限公司也推出了SSD控制芯片，支持AES 128/256、TCG Opal Full-Drive等加密机制。

Greenliant是由原SST（冠捷半导体）创始人Bing Yeh创立的一家快速成长的存储芯片、系统和方案提供商。公司前身为SST，其核心技术人员及管理层均来自SST的研发和市场部门。SST在2000年开始做BGA SSD，2010年把SSD业务卖给Greenliant，同年，Microchip收购SST。

硅格，成立于2007年，在闪存存储领域摸爬滚打近十年，也算是小有成绩。在2017年深圳举行的中国闪存市场峰会上，硅格半导体总经理吴大畏先生表示，10多年来，硅格累计出货数亿颗eMMC控制器等芯片。在SSD领域，尽管起步稍晚，但SATA的控制器很快就会面市。

威盛在北京的团队也从事SSD主控芯片研发，产品接口从SATA到PCIe 3.0都有，支持TLC闪存和LDPC纠错。

联芸，总部位于杭州，在台湾也有团队。它的前身是JMicron，囿于台湾不肯开放芯片设计业，索性把台湾的部门解散，到杭州来注册公司，成为自主品牌，以后会慢慢看不到智微的控制器了。以JMicron在SSD领域这么多年的积累，技术起点会高不少，但是关键要看老板想怎么玩，炬力就是前车之鉴。只要能让员工也能分享到公司发展的好处，就有机会发展起来。

Phison在合肥成立了兆芯，希望能落地开花。

还有一个大玩家是兆易创新，其上市之后，闪电买下忆正武汉SSD工厂。2016年4月新成立子公司上海睿磐电子信息技术有限公司，引入国内业界顶尖的技术团队，主要成员来自SSD控制器的传奇公司SandForce，专注于SSD研发。如果武汉长江存储的3D闪存能如期量产，以他们之前的合作关系，应该是最容易拿到颗粒的。这样品牌和颗粒都有了，不做SSD控制器就说不过去了。

深圳的新创SSD控制器公司大普微电子也是后起之秀，他们得到了深圳市的大力支持，同时产品支持人工智能等功能，很有特色。

国内还有不少知名SSD厂商的部分产品采用FPGA控制器方案，比如方一信息科技、宝存科技等。这些公司发展如何，还需要三五年后才能看出水平，但是只要能耐得住寂寞，坚持打磨产品，再配上良好的激励机制，还是很有可能成功的。

2.3 案例：硅格（SiliconGo）SG9081主控

本节以国产主控厂商硅格的SATA3.2SSD主控SG9081为例，剖析一下主控如何实现高性能。

图2-14为SG9081主控的结构框图。

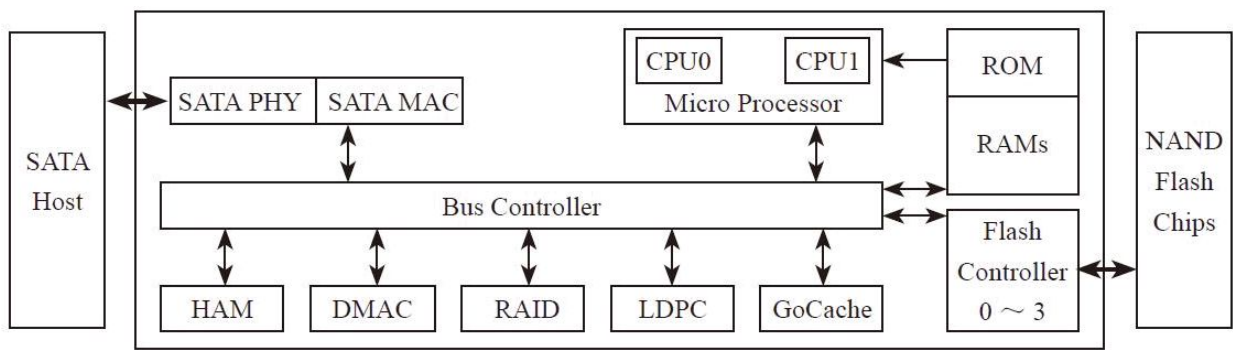


图2-14 SG9081主控的结构框图

1.HAM+GoCache加速随机读写的IOPS

HAM是硬件加速模块的简称，SSD主控中除了MCU以外，还有一个硬件加速模块HAM。该模块将部分算法处理的动作硬件化，一方面释放了MCU的资源，另外一个方面则加速了算法的实现，尤其是对小数据的处理。另外，主控中集成了GoCache（SiliconGo独有技术），可高效地实现映射关系的管理，从而更高效地提高对小数据的传输能力。两者的结合实现了SSD成品模组性能的提升。

2.DMAC加速顺序读写

DMAC是Direct Memory Access Controller的缩写。该模块的存在使得SSD在进行连续大数据传输的时候，不用一直占据MCU的资源。当DMA请求被发起时，内部总线裁决逻辑将交由DMAC控制，接着数据高速传输动作开启。传输过程中，MCU可以去处理其他的事务，而当数据传输结束之后，DMAC又会将总线让给MCU。在这样的机制保证下，SSD进行读写操作时的效率极大地提高，从而表现出优秀的顺序读写性能。

3.LDPC+RAID提高可靠性，增强闪存耐久度和数据留存能力

目前闪存正从2D转向3D架构，对闪存纠错处理的要求也越来越高，早期的BCH已经无法满足先进制程或先进工艺的闪存。SG9081主控采用LDPC实现ECC，LDPC码在相同的用户数据条件下，与BCH校验码相比能纠正更多的错误，同时也增强了闪存的使用寿命。而RAID功能的引进则给数据保护加上了一个双保险。主控中的RAID功能可以理解为给数据做了一层校验保护，必要的时候可以通过校验的内容恢复为原始数据。LDPC和RAID功能大大地提高了数据的稳定性。

2.4 案例：企业级和消费级主控需求的归一化设计

SSD有企业级与消费级之分。企业级SSD产品更加注重随机性能、延迟、IO QoS的保证及稳定性；而消费级产品则更加注重顺序性能、功耗、价格等，如表2-3所示。

表2-3 企业级和消费级SSD对比

	企业级	消费级		企业级	消费级
性能	随机敏感	顺序敏感	耐久度	10^{-16}	10^{-15}
生命周期	1 ~ 5 (DWPD)	500TWD	功耗（控制器）	5 ~ 10W	<2.5W
容量	0.6TB ~ 8TB	64GB ~ 1TB			

SSD控制器在设计时需要为企业级和消费级产品分别优化，这样不仅加大了研发成本，也增大了下游多系列SSD产品开发的复杂度。

是否有一款归一化的SSD控制器，能同时满足企业级和消费级需求？主要的问题在于能否在控制器硬件架构上实现成本、功耗和功能的统一。

1) 成本方面，企业级SSD对控制器成本较不敏感，归一化SSD控制器需要着重满足消费级SSD的成本预算。采用通用硬件架构并优化硬件资源开销来约束SSD控制器成本，通过差异化固件来满足企业级与消费级产品的不同性能需求。

2) 在性能方面，经过市场沉淀，NVMeU.2形态与M.2形态的SSD逐渐成为主流，两种形态的SSD产品性能需求也趋于一致。作为AIC形态的取代品，1U服务器普遍承载8块或更多U.2形态SSD，使得U.2形态SSD单盘4KB随机性能在300~400KIOPS，这已能满足大部分应用需求。反观消费级SSD市场，高端游戏平台NVMe M.2形态的SSD理论上性能已达3.5GB/s，这样的性能指标已与一些企业级SSD的顺序IO相近。一些互联网厂商已在IDC数据中心中应用M.2形态的SSD。在数据中心，上层对数据流做了大量优化，数据以顺序访问方式写入SSD，这降低了对企业级SSD随机性能的需求。

3) 在寿命上，企业级与消费级SSD需求差别较大。但影响SSD寿命的主要因素在于闪存的耐久能力。SSD控制器则确保加强对闪存的纠错能力。因此，企业级与消费级SSD控制器在寿命方面的设计目标是一致的。

4) 在容量上，企业级SSD与消费级SSD差异较大。SSD控制器需要以比较小的代价支持大容量闪存，以便同时覆盖企业级与消费级SSD的需求。

5) 可靠性方面，企业级SSD一般要求ECC与DIE-RAID两层数据保护能力。而随着3D闪存逐步普及，闪存厂商开始建议在消费级SSD上提供DIE-RAID能力。所以在可靠性方面，企业级与消费级SSD控制器的设计目标也趋于一致了。

6) 在功耗方面，消费级产品对功耗最为敏感，特别是像平板、笔记本电脑这种电池供电设备，对功耗有严格的限制。SSD控制器在设计时需要考虑复杂的低功耗需求，需要支持多种电源状态，以及快速唤醒。企业级SSD对功耗相对不敏感。然而对于整个数据中心，电力成本已占数据中心运营成本近20%。随着SSD的大规模部署，低功耗设计也成为企业级SSD控制器的追求目标。

从上面几点不难看出，在企业级与消费级SSD设计指标趋于一致的趋势下，硬件规格实现统一是极有可能的。而SSD产品形态的差异化则由SSD控制器上的固件体现。忆芯科技的STAR1000芯片在设计中对此做了比较成功的尝试，如图2-15所示。



图2-15 STAR1000关键技术

STAR1000固态硬盘控制器采用SMP架构，极大程度保留了硬件扩展性和软件灵活性，便于多种存储硬件加速模块的集成，降低了固件开发的复杂度，对实时OS有天然的良好支持。

可靠性方面，对片上SRAM、片外DRAM与数据通路都可进行错误校验，满足了企业级要求；用极小代价实现了RAID5/6保护机制；特别是通过RAID的校验RAM和片上SRAM共享设计，既能满足企业级SSD要求，也能在某些消费级产品不需要RAID机制时，将SRAM让给固件做其他事情，极大提升了资源利用率。

NVMe子系统采用2颗32位嵌入式CPU搭配NVMeIO硬件加速器方案，特别适合低功耗实现消费级SSD的基础IO性能要求，同时满足了企业级应用中对队列调度策略、高性能SGL实现、原子操作、HMB/CMB支持等特性，此外还支持多VF的SRIOV。

2.5 案例：DERA（得瑞领新）NVMe控制器TAI和NVMe SSD产品

NVMe协议面向现代多核计算系统结构设计，充分发挥NVM介质高并发及低延迟的特性，为实现高吞吐量、低延迟的存储设备打下了良好的生态基础。DERA Storage遵循协议标准，面向企业计算市场，开发提供高性能、高可靠的NVMe SSD解决方案。

控制器是NVMe SSD的核心部件，是连接主机总线和闪存单元的桥梁。本质上，一个NVMe SSD设备内部需要处理高并发的大量IO事务，每个IO事务都伴随多种硬件操作和事件处理，其中一些功能特性需要结合计算密集型的操作，比如用于数据错误检测的编解码，或者数据加密、解密，在完成这些处理的同时还要满足苛刻的功耗要求，因此不可避免地需要使用专用的硬件加速单元。综合考虑，NVMe SSD控制器一般是紧密结合NAND闪存管理软件进行高度定制化设计的ASIC（专用集成电路）。只有将数据通路、计算资源都经过合理安排调配，最终实现的NVMe SSD才能在可靠性、性能、功耗几个方面实现良好统一的目标。

DERA NVMe控制器是DERA NVMe SSD产品的核心部件，TAI是DERA的第一款控制器（见图2-16）。DERA TAI前端支持PCIe Gen3x8或x4接口，集成多个NAND接口通道和高强度ECC硬件编解码单元，所有数据通道均运用ECC和CRC多重硬件保护机制。在TAI控制器基础上，紧密协同设计的闪存转换层（FTL）算法负责调度管理，综合运用多种技术实现企业级的数据存储可靠性，充分发挥NAND闪存的高速存取特点，实现高可靠、低延时、高吞吐量的数据存储要求。

DERA NVMe SSD定位于企业级应用，因此性能平稳度和数据可靠性是核心的设计要点。

企业级应用要求存储设备在稳定一致的基础上具备高性能和低延迟的特性。受限于介质的基本工作原理，SSD需要通过复杂的工程设计才能避免出现性能抖动、延迟时间恶化等负面表现。DERA企业级NVMe SSD充分预计了高压下的极端情况，对前端IO请求和后台行为进行精细调度和控制，确保在任何情况下，设备对外呈现的性能都能稳定在可预测、可接受的水平。

在数据可靠性方面，DERA产品主要通过高强度的硬件ECC、故障主动管理、完整数据通道校验、掉电保护、功耗及温度自监控管理等技术设计实现。

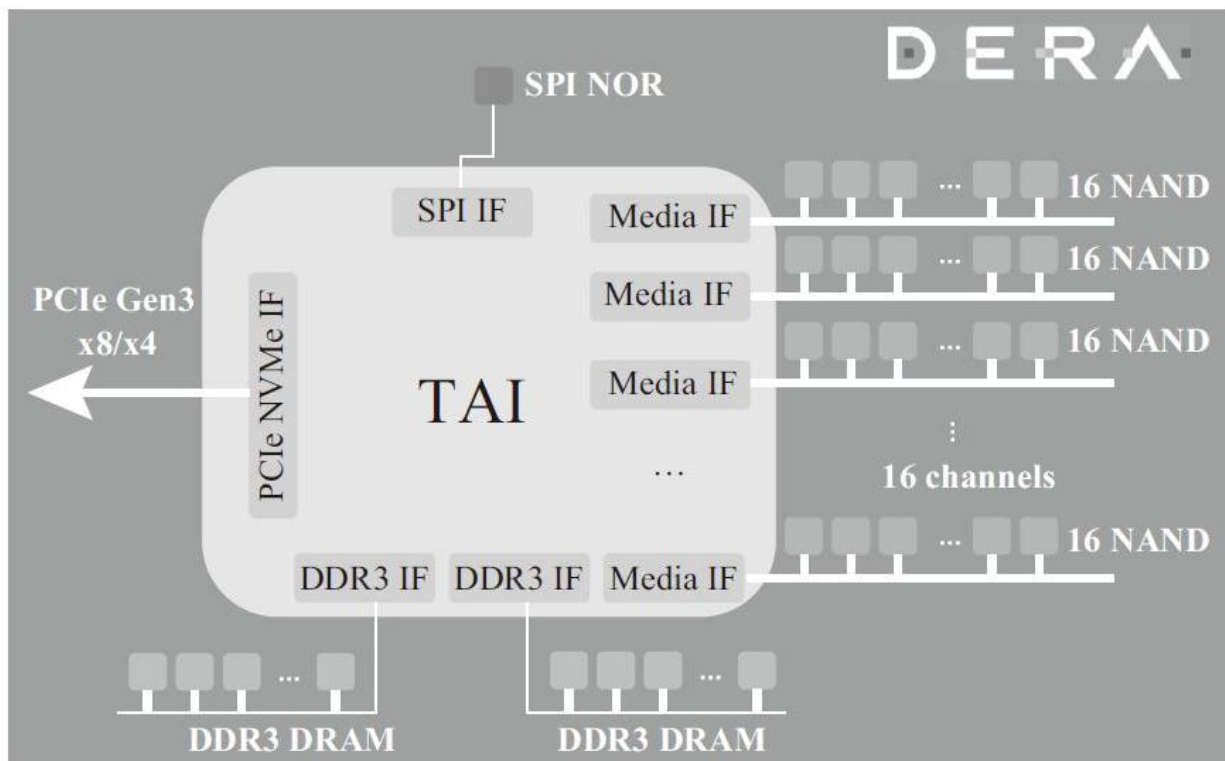


图2-16 DERA TAI控制器

闪存ECC是SSD的核心功能。为了处理新结构、新工艺节点下闪存芯片的高原始误码率，以及满足高并发访问时的低延迟要求，DERA TAI控制器为每个闪存通道都配备了独立的ECC单元，纠错能力为100b/1KB，满足主流闪存器件对主控纠错能力的要求，即在复杂度、面积和功耗、解码延迟时间确定性和可控性等多个方面达到了良好的均衡。此外，DERA TAI对完整数据通道的ECC保护和CRC校验，也在不影响性能的前提下为数据可靠性提供了进一步的基础保障。

闪存存储单元在形成严重错误之前会表现为误码率的渐进式提高。**DERA SSD**在充分掌握闪存器件全生命周期特性的基础上，在运行过程中根据页面原始误码率的变化，实现对故障单元的主动判定及预防性的管理策略，在最大化有效使用存储单元的基础上，最大限度降低因存储单元故障导致的数据损坏的概率。与此对应，磨损平衡策略也基于对存储单元的实时跟踪结果而动态调整，确保达到更接近真实情况的磨损平衡效果。

企业级SSD另外一个非常重要的系统级数据保护机制就是闪存芯片之间的冗余校验机制。**DERA SSD**将多个不同闪存芯片上的存储单元按照一定大小进行划分，组成动态组合的冗余校验结构。如果某个芯片上的数据块出现错误，管理算法能够基于其他芯片上的数据块重新构建出错芯片上的数据，并对出错的芯片物理单元做妥善处理。

在IT系统运行环境下，意外掉电是不可避免的问题。**SSD**对意外掉电若处理不当，很大可能会导致用户数据被破坏乃至整个设备出现故障。**DERA SSD**提供完备的硬件手段持续监测供电情况，并在供电异常时触发保护策略，自动切换到后备电容或其他不间断电源供电，在整体的软件策略上予以充分配合，在发生意外掉电时最大限度保证用户数据的完整性。

NVMe SSD是高性能设备（见表2-4），虽然能提供优越的性能功耗比，但是在高负载情况下其功率消耗和相应的发热量也是不能忽视的问题。受限于安装密度、系统风道的设计，以及系统风扇管理策略在一定阶段内的局限性，在某些安装条件下，**SSD**设备有可能会面临散热风量不足的问题。**DERA SSD**在运行过程中持续监测设备温度及功率使用情况，并按照预定策略动态处理，确保不会因为系统散热条件不足而导致设备故障或更严重的问题。

表2-4 DERA NVMe SSD性能

	DERA NVMe SSD (Gen3x4)	DERA NVMe SSD (Gen3x8)		DERA NVMe SSD (Gen3x4)	DERA NVMe SSD (Gen3x8)
顺序写入	3.4GB/s	4.5GB/s	随机写入	270k IOPS	270k IOPS
顺序读取	3.4GB/s	5.1GB/s	随机读取	760k IOPS	1.17M IOPS

2.6 全闪存阵列AFA

经常听人说起全闪存阵列，给人一种很厉害的样子，那这个全闪存阵列到底是个什么东西？下面将以某一款EMC XtremIO为例来带你入门。

本节参考了Vijay Swami写的XtremIO Hardware/Software Overview&Architecture Deepdive一文，图片也主要来自这篇文章。

2.6.1 整体解剖

1.结构

图2-17所示是一个标准的XtremIO全闪存阵列，含有两个X-Brick，之间用Infiniband互联。可以看出，X-Brick是核心，那么X-Brick里面究竟是什么？

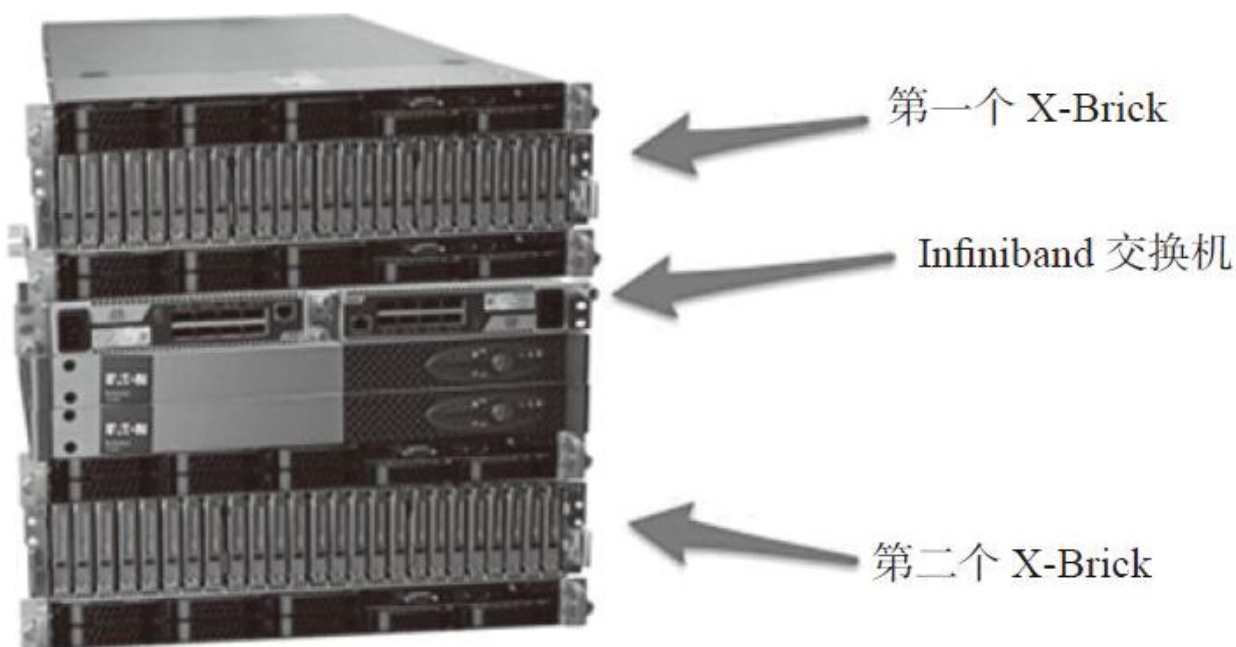


图2-17 XtremIO全闪存阵列结构

我们来看看，一个X-Brick包括：

- 1个高级UPS电源；
- 2个存储控制器；

·磁盘阵列存储柜DAE，放有很多个SSD，每个SSD都用SAS连接到存储控制器；

·如果系统有多个X-Brick，那么需要2个Infiniband交换机来实现存储控制器高速互联。

2.存储控制器

如图2-18所示，存储控制器其实就是个Intel服务器，配有2个电源，看起来是NUMA架构的2个独立CPU、2个Infiniband控制器、2个SAS HBA卡。Intel E5CPU，每个CPU配有256GB内存。



图2-18 存储控制器机箱内部

如图2-19所示，其后面插有各种线缆，看着感觉乱糟糟的，如图2-19所示。设计的架构适用于集群，所以线缆有很多是冗余的。



图2-19 X-Brick背面连线图

阵列正面照，LCD显示的是UPS电源状态。图2-20所示是一个个竖着的就是SSD阵列。



图2-20 Xtrem-IO全闪存阵列正面照片

3.配置

如表2-5所示，一个X-Brick容量是10TB，可用容量7.5TB，但是考虑到数据去重和压缩大概为5:1的比例，最终可用容量为37.5TB。

表2-5 XtremIO配置表

	1 个 X-Brick	2 个 X-Brick 集群	4 个 X-Brick 集群	8 个 X-Brick 集群
组件	2 个 X-Brick 控制器 1 个 X-Brick DAE 2 个备用电源	4 个 X-Brick 控制器 2 个 X-Brick DAE 2 个备用电源 2 个 Infiniband 交换机	8 个 X-Brick 控制器 8 个 X-Brick DAE 8 个备用电源 2 个 Infiniband 交换机	16 个 X-Brick 控制器 8 个 X-Brick DAE 8 个备用电源 2 个 Infiniband 交换机
功耗 (W)	750	1 726	3 226	6 226
空间 (U)	6	13	23	43
制冷需求 (BTU/h)	2 559	5 889	11 000	21 244
物理容量 (TB)	10	20	40	80
可用容量 (TB)	7.5	15	30	60
去重压缩后容量 (TB)	37.5	75	150	300

4.性能

有人做了XtremIO性能测试，在2个X-Brick的全闪存阵列跑了550个虚拟机，为7000个用户服务器提供服务。其每天平均读写带宽为350MB/s~400MB/s，20k IOPS；最高时达到20GB/s，200k IOPS。

5.软件控制台

我们来看看软件控制台参数，如图2-21所示，图左边显示数据降低率2.5: 1，其中去重率1.5: 1，压缩率1.7: 1；图右边是带宽、IOPS和延迟监控图，显示每个SSD当前的性能和汇总的读写性能。



图2-21 软件控制台性能监控

图2-22是每个SSD的监控图，DAE中每个盘下面有模拟的灯，根据盘当前的读写活动不断闪烁，看起来非常酷！

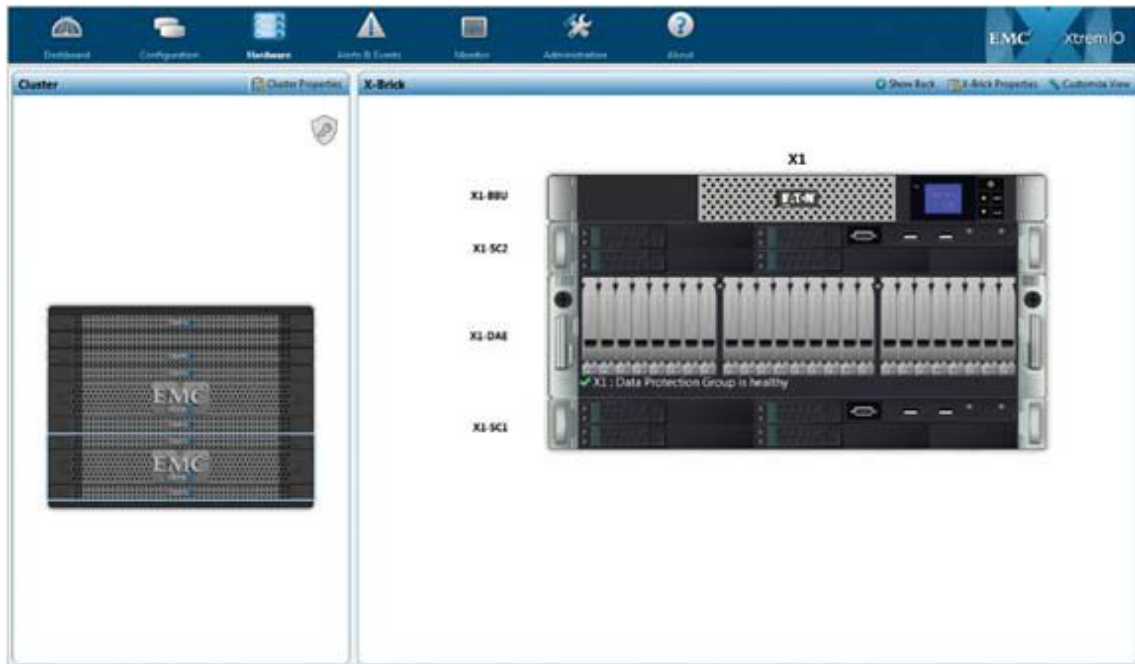


图2-22 SSD监控图

2.6.2 硬件架构

EMC XtremIO是EMC对全闪存阵列市场的突袭，它从底层开始完全根据闪存特性设计。

如图2-23所示，1个X-Brick包含2个存储控制器，一个装了25个SSD的DAE，还有2个电池备用电源（Battery Backup Unit，BBU）。每个X-Brick包含25个400GB的SSD，原始容量10TB，使用的是高端的eMLC闪存，一般擦写寿命比普通的MLC长一个数量级。如果只买一个X-Brick，配有两个BBU，其中一个是为了冗余。如果继续增加X-Brick，配有两个BBU，其中一个是为了冗余。如果继续增加X-Brick，那么其他的X-Brick只需要一个BBU。



图2-23 X-Brick尺寸

X-Brick支持级联来增加容量，所以其是一种Scale-Out架构，最多可以到4个X-Brick甚至8个X-Brick（见图2-24）。

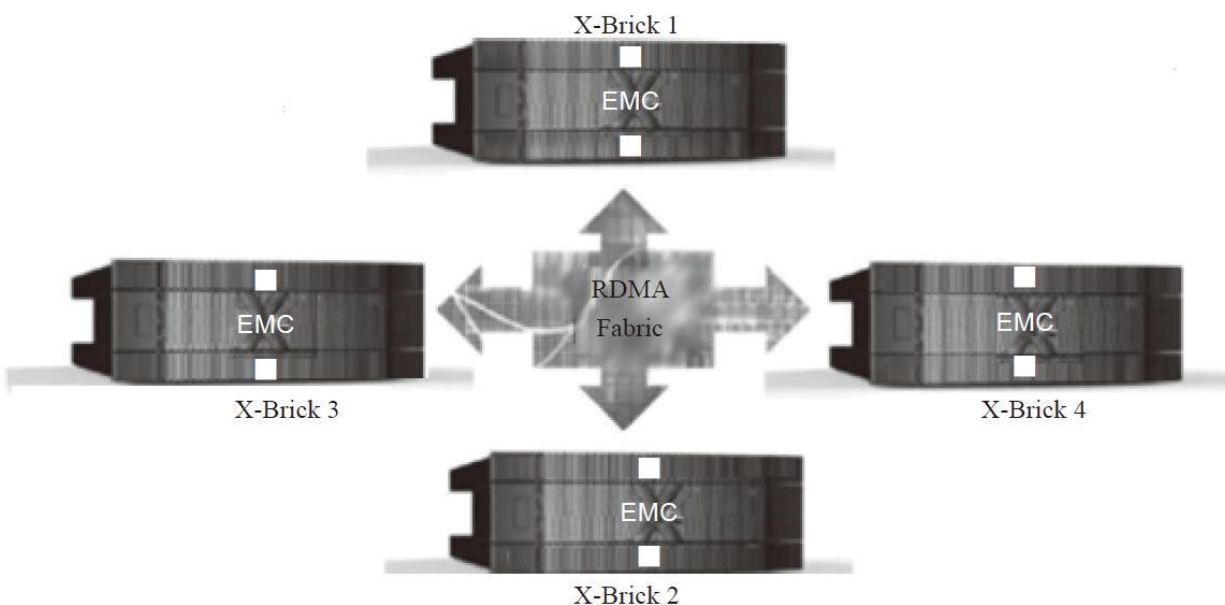


图2-24 X-Brick互联

X-Brick之间采用40Gbps的Infiniband交换机互联。

图2-25所示是一个X-Brick存储控制服务器的所有端口，40Gbps Infiniband接口是为了后端数据连接，其实就是X-Brick之间的互联。那么，阵列和主机控制端如何进行数据交互呢？可以看出，既可以使用8Gbps FC，也可以使用10Gbps的iSCSI。那又是如何连到那么多的SSD上呢？用的是6Gbps的SAS接口，和VNX类似。同时，电源和所有的接口都是有冗余的，用来应对故障。那么一个X-Brick节点自己数据的存储如何解决呢？它配有2个SSD，用来掉电时保存内存中的元数据。要知道，去重还是很占用内存的，因为一般每个数据块需要计算出一个Hash值，甚至双重Hash，用Hash值来判断唯一性。同时还有2个SAS硬盘，作为操作系统运行的磁盘。

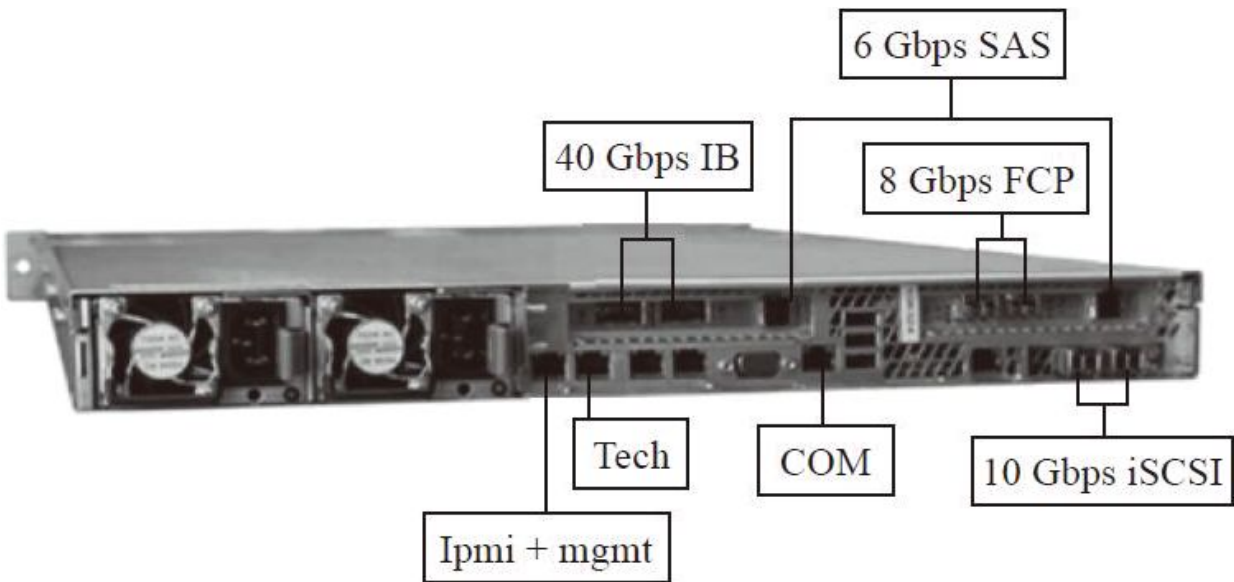


图2-25 X-Brick存储控制器端口

这样一来，存储控制器有自己的硬盘，而不占用DAE里面的SSD阵列，闪存阵列只用于存储用户数据，受2个存储控制器管理。这种架构的好处是结构清晰、界限分明，未来还能直接升级存储控制器软硬件而不动闪存阵列里的数据。

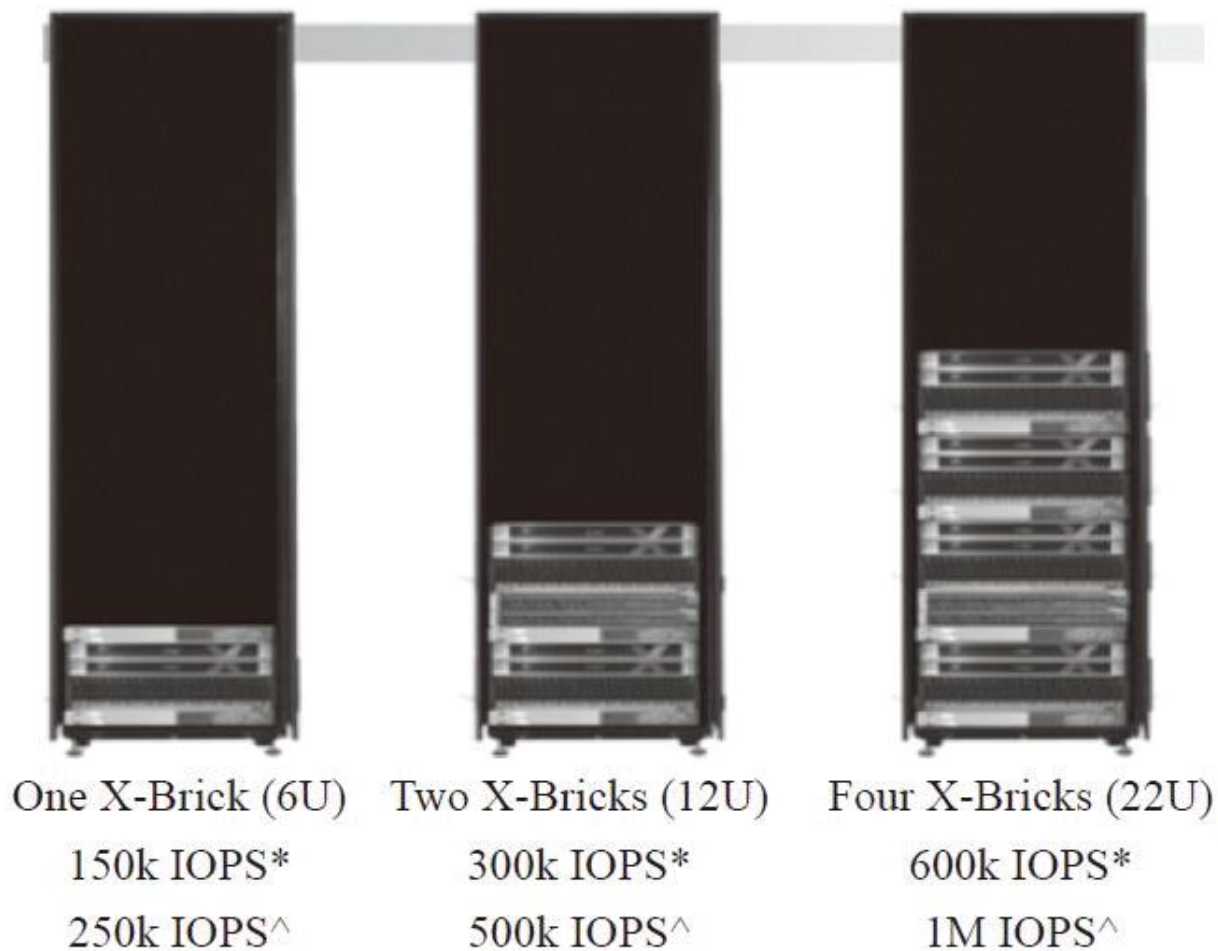
再来看看每个存储控制器的配置：有2个CPU插槽的1U机箱，使用2个8核的Intel Sandy Bridge CPU，256GB内存。

现在很多厂商都以最高性能为荣，拿一个新盘，写一点数据，甚至往DRAM Cache里面写一点然后读出来，就吹嘘带宽、IOPS、延迟达到什么程度。更有甚者，不写数据，空盘读，达到巅峰带宽，简直把用户当三岁小孩。殊不知，对用户来讲，尤其是企业级用户，最高性能说明不了什么，只能忽悠那些不懂行的人，对真正业内人士来说，实际使用的稳定性能才是王道。

EMC全闪存阵列XtremIO，1个10TB的X-Brick，可用容量只有7.5TB，但是考虑到数据去重，用户能用的容量其实很大，跟实际的应用相关。比如虚拟桌面VDI应用，数据重复率很高，想想不同人安装的Windows XP虚拟机的系统文件基本都是一样的，去重可以省下多大的空间啊！但是像一般的数据库应用，重复率又很低，毕竟数据库存储的数据几乎是随机的。

我们来看看一个X-Brick的IOPS（见图2-26）：

- 100%4KB写： 100k IOPS °
- 50/504KB读/写： 150k IOPS °
- 100%4KB读： 250k IOPS °



*IOPS 测量标准：4K 随机访问，读写比 50%：50%

^IOPS 测量标准：4K 随机访问，100% 全读操作

图2-26 XtremIO性能

如果是2个或更多X-Brick级联，性能线性增长，前面的数值翻几倍就可以了。

有一点必须得强调，上面说的这个性能看起来一般，但是要知道，这可是实际使用的性能，而且不是空盘拿来跑跑的性能，而是全盘写了至少80%之后的性能。为什么要写至少80%才能测得真正的性能？因为空盘写不会触发垃圾回收，当用户占满了整个带宽，且盘快写满的时候，垃圾回收才开始工作，此时用户能分到的带宽就少了，性能自然下降。而我们买了盘，肯定很快会写很多数据，所以只有快写满了才是常态。

2.6.3 软件架构

存储行业发展到今天，硬件越来越标准化，所以已经很难靠硬件出彩了。若能够制造存储芯片，例如三星这种模式，从底层开始都自己做，则可靠巨大的出货量坐收硬件的利润。但这种模式投资巨大，一般人玩不来，只能靠软件走差异化了，而且软件还有一个硬件没有的优势：非标准化。比如IBM的软件很多是基于自己的UNIX系统开发的，别人用了之后切换到其他厂家的软件难度很大，毕竟丢数据的风险不能随便冒。

看了前面的XtremIO（XIO）硬件架构之后，不少人可能觉得并没有什么复杂的，基本上就是系统集成、组装机嘛。但是，全闪存阵列的核心在软件，软件做好了，才能让用户体验到闪存阵列的性能。试想，如果iPhone装的是Android系统，你还会排队花五六千元去买吗？估计连两三千都舍不得了吧！



图2-27 装了Android的iPhone

1.XIO软件几大杀器

·去重：提升性能，同时因为写放大降低，延长了闪存的寿命，提高了可靠性。

- Thin Provisioning**: 分区的容量可以随着使用而自动增长（直到用满阵列），这样关键时刻不会影响性能。

- 镜像**: 先进的镜像架构保证了容量和性能不会受损。

- XDP数据保护**: 用**RAID6**保护数据。

- VAAI集成**: 后面解释这是个什么。

2.XIO软件核心设计思想

1) 一切为了随机性能: 任何节点上访问任意数据块, 都不会增加额外的成本, 即必须公平访问所有的资源。这是为什么? 这样的结果就是即使节点增加, 性能也能够线性增长, 扩展性也好。

2) 尽可能减少写放大: 要知道, 对**SSD**来讲写放大不仅会导致寿命缩短, 还会因为闪存的擦写次数升高, 导致质量下降, 数据可靠性下降。**XIO**的设计目标就是让后台实际写入的数据尽量少, 起到一种数据衰减的作用。

3) 不做全局垃圾回收: **XIO**使用的是**SSD**阵列, 而**SSD**内部是有高性能企业级控制器芯片的, 当前的**SSD**主控都非常强大, 垃圾回收效率很高, 所以**XIO**并没有再重复做一遍垃圾回收。这样做的效果是降低了写放大, 毕竟后台搬移的数据量少了, 同时, 节省出时间和系统资源提供给其他软件功能、数据服务和**VAAI**等。

4) 按照内容存放数据: 数据存放的地址用数据内容生成, 跟逻辑地址无关。这样数据可以存放在任何位置, 提升随机性能, 同时还可以针对**SSD**做各种优化。数据可以平均放置在整个系统中。

5) **True Active/Active**数据访问: **LUN**没有所有者一说, 所有节点都可以为任何卷服务, 这样就不会因为某一个节点出问题而使性能受损。

6) 扩展性好: 性能、容量等都可以线性扩展。

3.XIO软件为什么运行在Linux用户态?

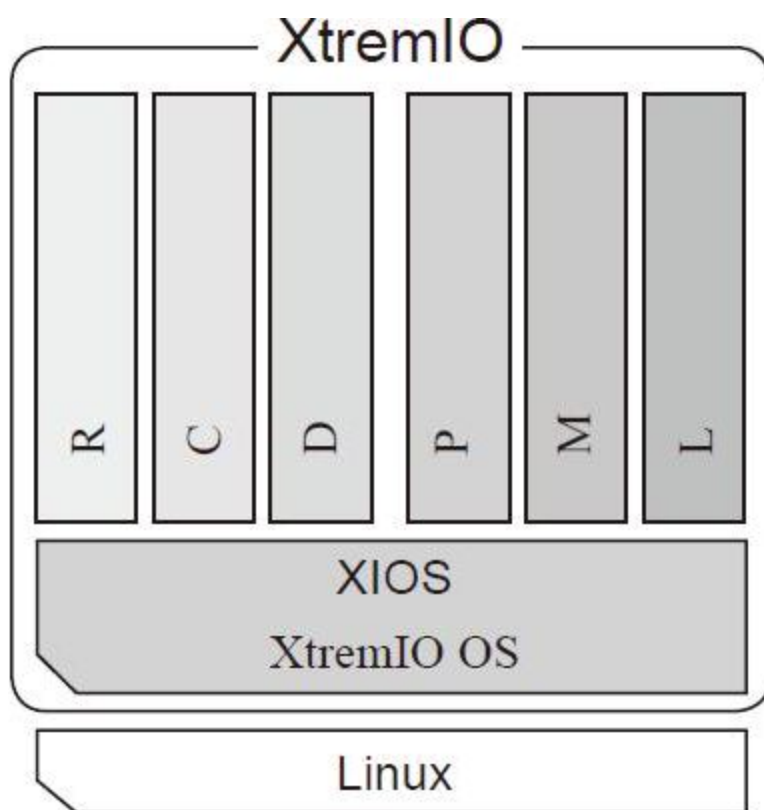


图2-28 XIO软件架构

如图2-28所示，XIO的全闪存阵列软件架构，XIO OS和XIO的软件都运行在Linux的用户态，这样有什么好处呢？我们知道，Linux系统分为内核态和用户态，我们的应用程序都在用户态运行，各种硬件接口等系统资源都通过内核态管理，用户态通过system call访问内核资源。XIO软件运行在用户态有几大优点：

- 避免了内核态的进程切换，速度快。
- 开发简单，不需要借助各种内核接口，以及复杂的内存管理和异常处理。
- 不必受到GPL的约束。Linux是开源系统，程序在内核运行必然要用到内核代码，按照GPL的规定，就得开源，在用户态自己开发的应用就不受此限制。这种商业性软件，里面很多东西都是公司花了很多心血开发的核心技术，开源了就太不值了。由此也可以看出软件对全闪存阵列的价值！开源了还能卖那么贵吗？或者说开源了，谁都可以组装起来，装一个开源软件，全闪存阵列就只能打价格战了，高科技当大白菜卖。

在每个CPU上运行着一个XIOS程序：X-ENV，如果你敲一下“top”命令，就会发现这个程序掌控所有的CPU和内存资源。为什么这么做？

第一个作用就是为了XIO能100%使用硬件资源，能够运筹帷幄之中，决胜千里之外。知道自己赚多少钱，才能想清楚该怎么花。

第二个作用是不给其他进程影响XIO性能的机会，保证性能的稳定。

第三个作用是提供了一种可能性：未来可以简单修改就移植到UNIX或者Windows平台，或者从X86CPU移植到ARM、PowerPC等CPU架构，因为这都是上层程序，不涉及底层接口。

XIO是完全脱离了硬件的软件，为什么这么说？因为他们被EMC收购之后，很快就从自己的硬件架构切换到了EMC的白盒标准硬件架构，说明其软件基本不受硬件限制。而且，XIO的硬件基本没有自己特殊的组件，不包含FPGA，没有自己开发的芯片、SSD卡、固件等，用的都是标准件。这样做的好处是可以使用最新、最强大的X86硬件，还有最新的互联技术，比如比Infiniband更快的技术。如果自己开发了专用的硬件，要跟着CPU一起升级就很麻烦了，总是会慢一拍。

甚至，XIO完全可以只卖软件，只不过目前EMC没这么干而已。现在是硬件、软件、EMC客户服务一起卖。没准哪天，硬件不赚钱了，EMC就只卖XIO软件了。

2.6.4 工作流程

1.6大模块

XIO软件分为6个模块，以实现复杂的功能，其中包括三个数据模块R、C、D，三个控制模块P、M、L。

- P（Platform，平台模块）：监控系统硬件，每个节点有个P模块在运行。

- M（Management，管理模块）：实现各种系统配置。通过和XMS管理服务器通信来执行任务，比如创建卷、LUN的掩码等从命令行或图形界面发过来的指令。有一个节点运行M模块，其他节点运行另一个备用M模块。

- L（Cluster，集群模块）：管理集群成员，每个节点运行一个L模块。

- R（Routing，路由模块）：

- 其实就是把发过来的SCSI命令翻译成XIO内部的命令。

- 负责来自两个FC和两个iSCSI接口的命令，是每个节点的出入口“看门大爷”。

- 把所有读写数据拆成4KB大小。

- 计算每个4KB数据的Hash值，用的是SHA-1算法。

- 每个节点运行一个R模块。

- C（Control，控制模块）：

- 包含了一个映射表：A2H（数据块逻辑地址——Hash值）。

- 具备镜像、去重、自动扩容等高级数据服务。

- D（Data，数据模块）：

- 包含了另一个映射表：H2P（Hash值——SSD物理存放地址）。可见，数据的存放地址跟逻辑地址无关，只跟数据有关，因为hash值是通过数据算出来的。

- 负责对SSD的读写。

- 负责RAID数据保护技术——XDP（XtremIO Data Protection）

2.读流程

读流程如下：

- 1) 主机把读命令通过FC或iSCSI接口发送给R模块，命令包含数据块逻辑地址和大小。
- 2) R模块把命令拆成4KB大小的数据块，转发给C模块。
- 3) C模块查A2H表，得到数据块的Hash值，转发给D模块。
- 4) D模块查H2P表，得到数据块在SSD中的物理地址，读出来。

3.不重复的写流程

不重复的写流程如下（见图2-29）：

- 1) 主机把写命令通过FC或iSCSI接口发送给R模块，命令包含数据块逻辑地址和大小。
- 2) R模块把命令拆成4KB大小的数据块，计算出Hash值，转发给C模块。
- 3) C模块发现Hash值没有重复，所以插入自己的表，转发给D模块。
- 4) D模块给数据块分配SSD中的物理地址，写下去。

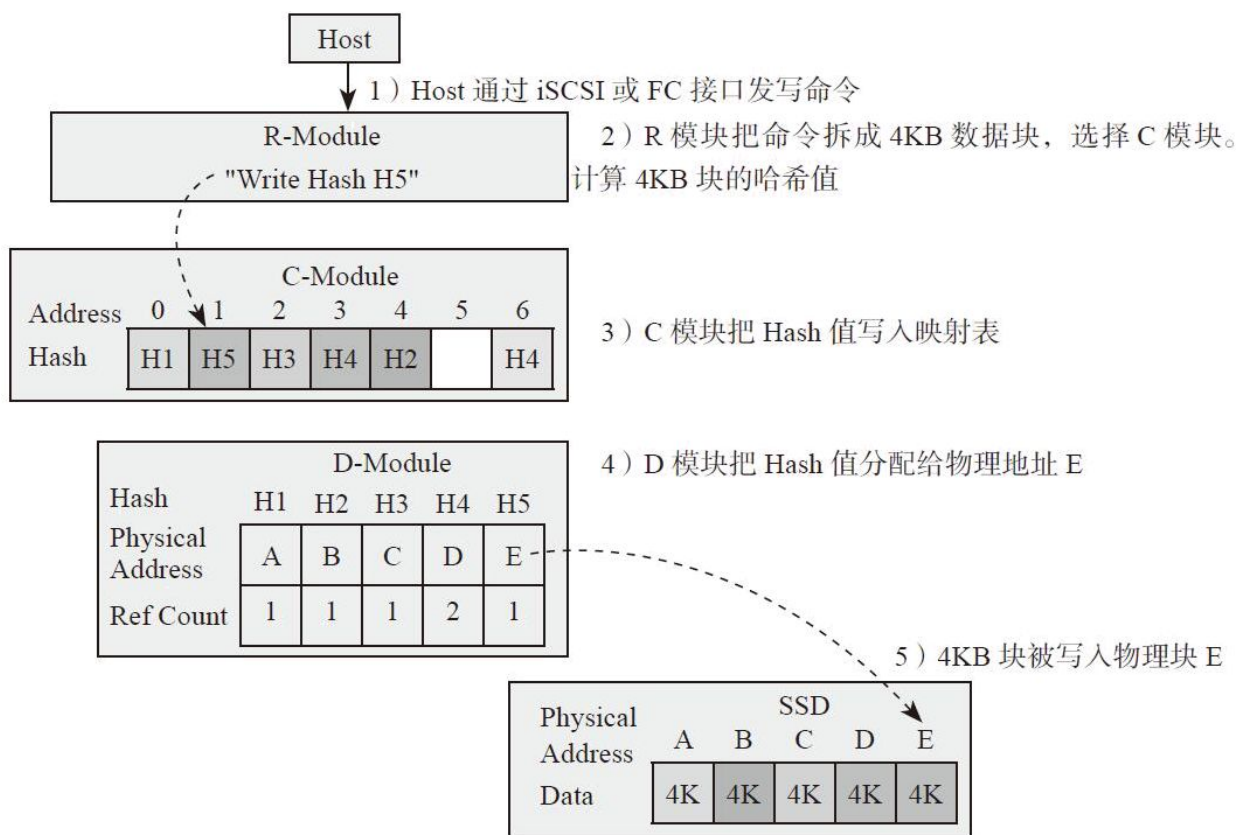


图2-29 不重复的写流程

4.可去重的写流程

可去重的写流程如下（见图2-30）：

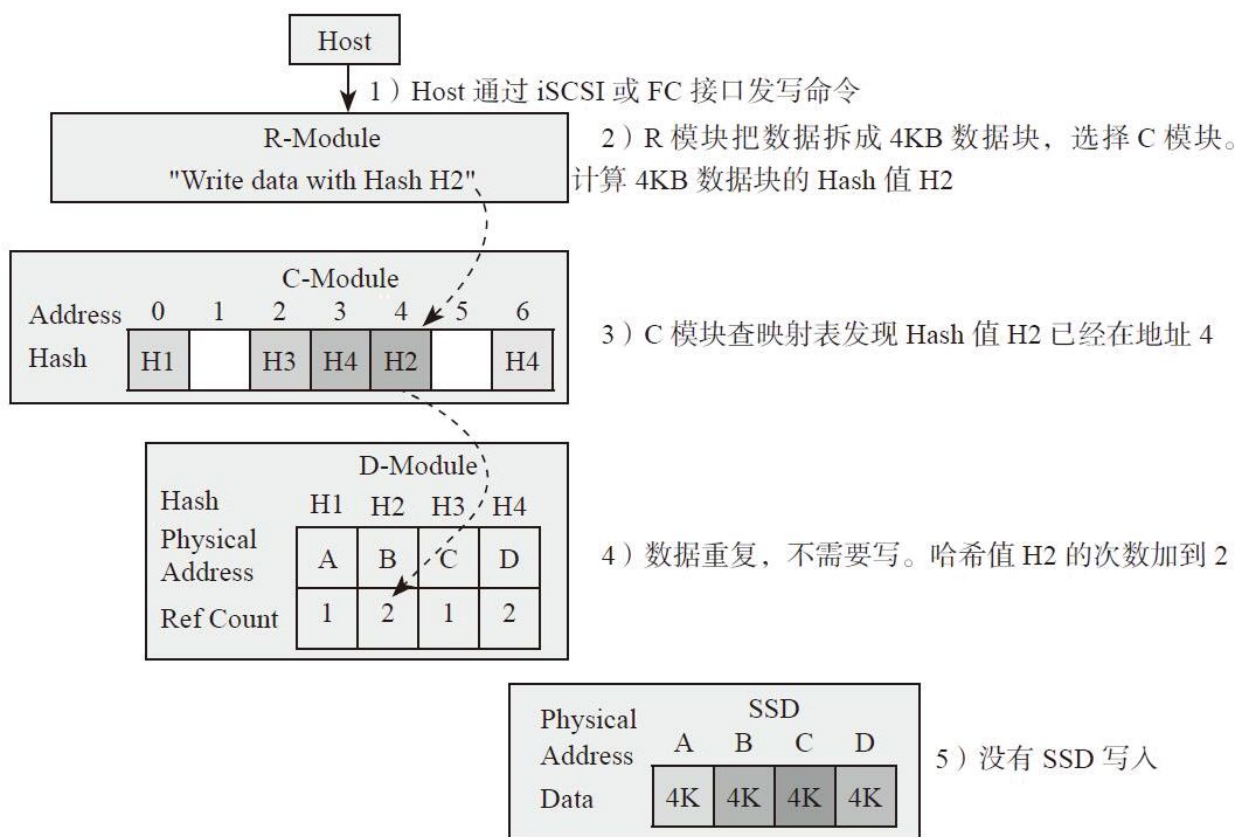


图2-30 可去重的写流程

1) 主机把写命令通过FC或iSCSI接口发送给R模块，命令包含数据块逻辑地址和大小。

2) R模块把命令拆成4KB大小的数据块，计算出Hash值，转发给C模块。

3) C模块查A2H表（估计还有个H2A表，或者是个树、Hash数组之类），发现有重复，转发给D模块。

4) D模块知道数据块有重复，就不写了，只是把数据块的引用数加1。

可以看出，自动扩容和去重都是在后台自然而然完成的，不会影响正常读写性能。

我们可以畅想整合了文件系统inode表和SSD映射表之后，复制会很简单，只需要两个逻辑块对应到一个物理块就可以了，并不需要读

出来再写下去。要知道自从全闪存阵列有了去重功能之后，复制这个基本的文件操作竟然如此简单：没有数据搬移，仅仅是某几个计数登记一下而已。下面我们细细道来。

5.ESXi和VAAI

首先我们来解释一下ESXi和VAAI两个名词。

VMware的虚拟化产品，就个人、小企业而言，有Workstation、ESXi（vSphere，免费版）、VMware Server（免费版）可以选择，Workstation和VMware Server需要装在操作系统（如Windows或Linux）上，ESXi则内嵌在操作系统中。所以ESXi可以看成是虚拟机平台，上面运行着很多虚拟机。

VAAI（vStorage APIs for Array Integration）是虚拟化领域的标准语言之一，其实就是ESXi等发送命令的协议。

6.复制流程

图2-31所示是复制前的数据状态。

复制流程（见图2-32）如下：

- 1) ESXi上的虚拟主机用VAAI语言发了一个虚拟机（VM）复制的命令。
- 2) R模块通过iSCSI或FC收到了命令，并选择一个C模块执行复制。
- 3) C模块解析出命令内容，把原来VM的地址范围0～6复制到新的地址7～D，并把结果发送给D模块。
- 4) D模块查询Hash表，发现数据是重复的，所以没写数据，只把引用数增加1。

这样复制完成了，没有真正的SSD读写。

不过有个问题是，这些元数据操作都是在内存中完成的，那万一突然掉电了怎么办？XIO设计了一套非常复杂的日志机制：通过RDMA

把元数据的改动发送到远端控制器节点，使用XDP技术把元数据更新写到SSD里面。XIO的元数据管理是非常复杂的，前面讲的流程只是简单介绍而已。

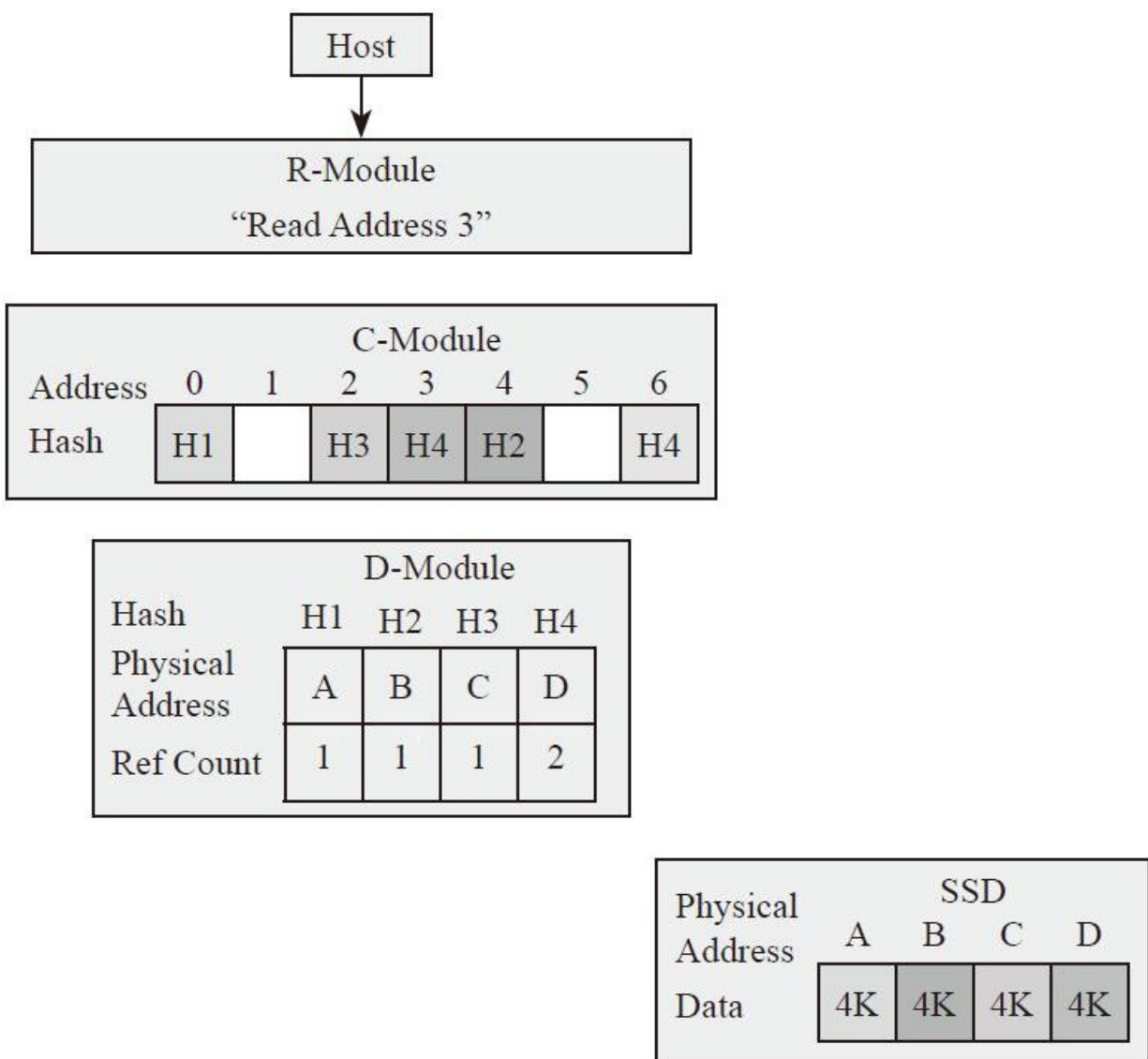


图2-31 复制前的数据状态

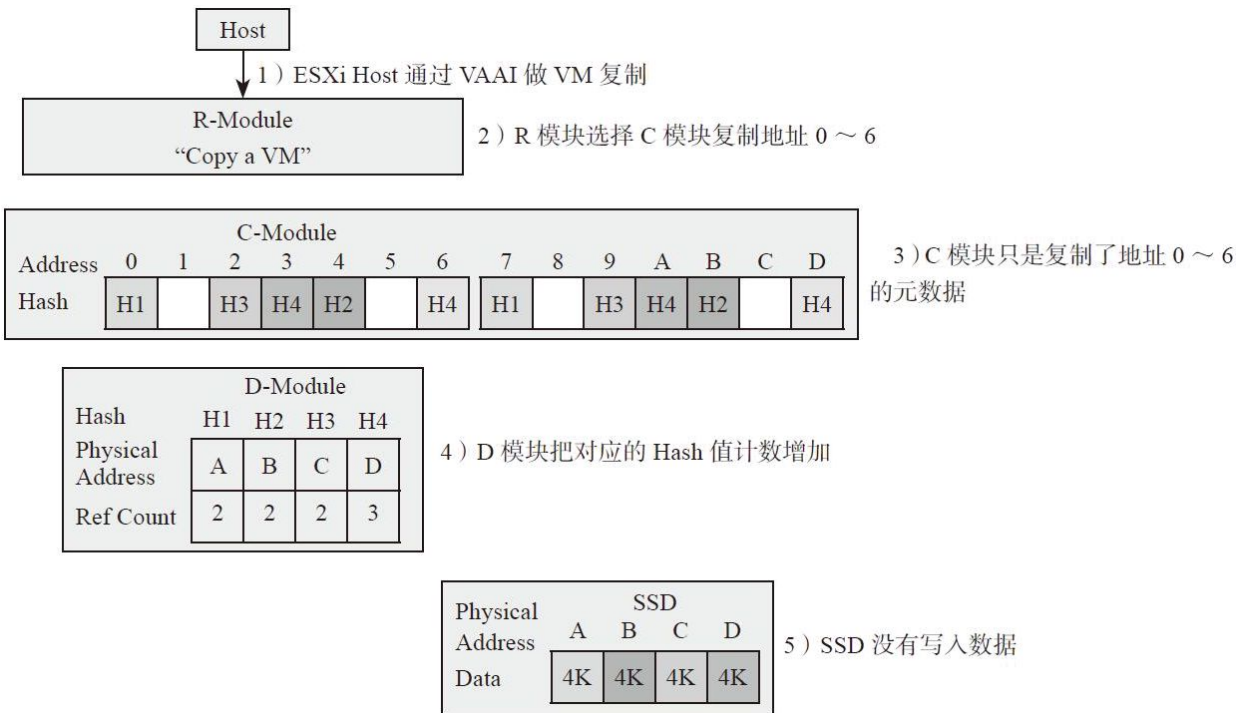


图2-32 复制流程

由于使用了A2H、H2P两张表，数据可以写到SSD阵列的任何一个地方，因为只跟数据的Hash有关，跟逻辑地址没关系。

最近网友们在热追中国高铁十三五规划，尤其是福建到台北的海底高铁更是令人震撼。短短十多年的时间，中国居然成为了世界第一高铁大国，乘坐高铁成为了大家城市间出行的第一选择。那为什么中国这么热衷于建设高铁呢？

人多！就是因为中国人口众多，而且稠密，基本集中在东部地区，比如京沪线，普通铁路的运力根本无法满足这么多人的需求，飞机也没办法拉完这么多人。高铁速度快，自然单位时间内能运载更多的人，交通效率更高。

在存储领域也是这个道理，全闪存阵列底层采用了闪存，所以速度很快，为了不浪费闪存的速度，上层的通信也需要非常高效。下面揭秘XIO全闪存阵列的内部通信。

7.回顾R、C、D模块

前文介绍了R、C、D三个数据相关的模块。

可以看出，R和上层打交道，C是中间层，D和底层SSD打交道，记住这个就可以了。

首先要搞清楚的是，这些模块物理上怎么放在控制服务器里面。前面说过，1个X-Brick的控制服务器有2个CPU，每个CPU运行一个XIOS软件。如图2-33所示，R、C模块运行在一个CPU上，D则运行在另一个CPU上。为什么要这么做呢？

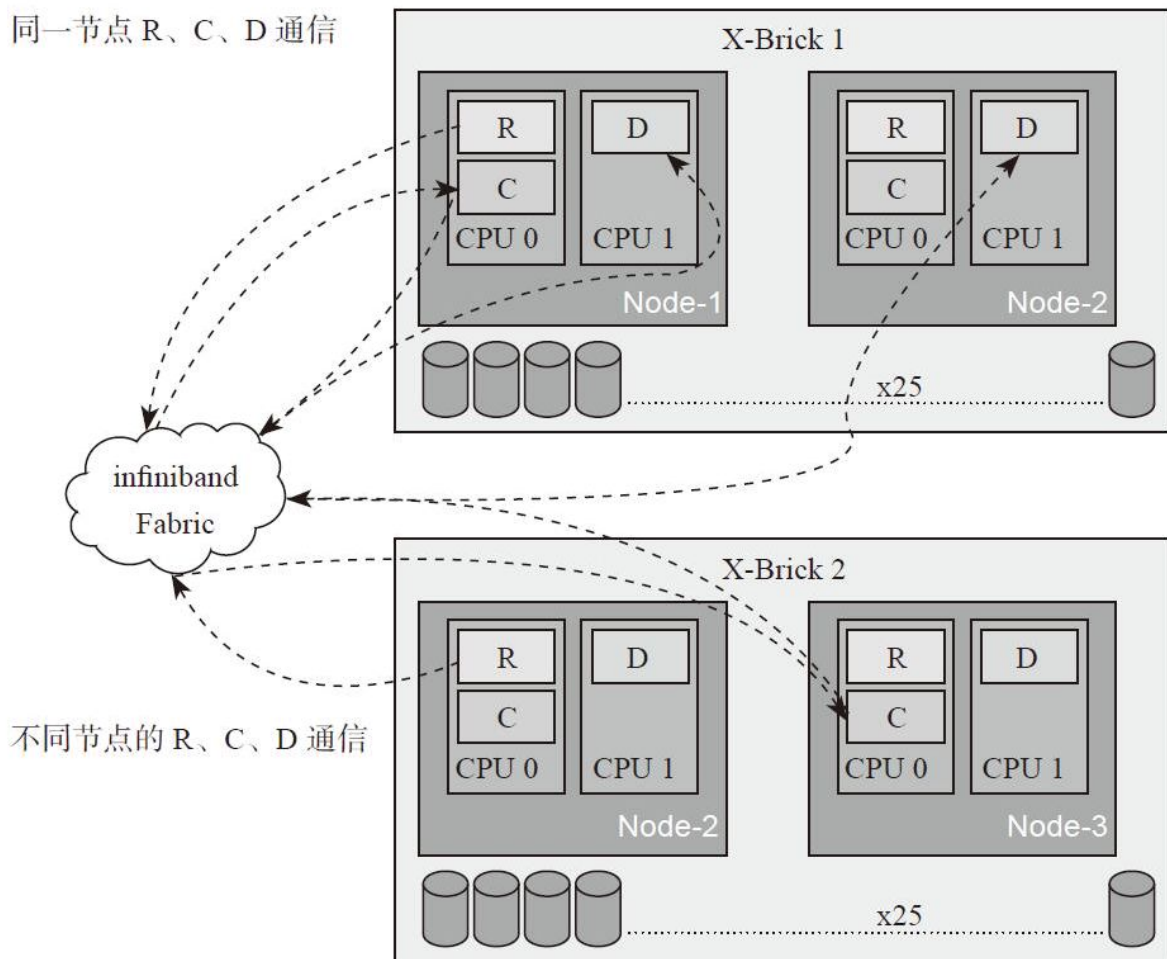


图2-33 X-Brick内部互联图

因为Intel Sandy Bridge CPU集成了PCIe控制器（Sandy Bridge企业版CPU集成了PCIe 3.0接口，不需要通过南桥转接）。所以，在多CPU的架构中，让设备直连CPU的PCIe接口，性能就会很高，而R、C、D的分布也是按照这个需求来设计的。例如SAS转接卡插到了CPU 2的PCIe插槽上，所以D模块就要运行在CPU 2上，这样性能才能达到最优。从这里，我们又可以看出XIO的架构上的优点，就是软件完全可以

按照标准化硬件来配置，通过布局达到最优的性能。如果CPU的分布变化了，也会根据新的架构简单调整软件分布来提升性能。

8.模块间通信：扩展性极佳

我们再来说说正题：模块间如何通信？其实并不要求模块必须在同一个CPU上，就像图2-33所示一样，R和C并不一定要在一个CPU上才行。所有模块之间的通信通过Infiniband实现，数据通路使用RDMA，控制通路通过RPC实现。

我们来看看通信的时间成本：XIO的IO总共延时是600~700 μ s，其中Infiniband只占了7~16 μ s。使用Infiniband来互联的优点是什么？其实还是为了扩展性，X-Brick即使增加，延迟也不会增加，因为通信路径没变化。任意两个模块之间还是通过Infiniband通信，如果系统里面有很多R、C、D模块，当一个4KB数据块发到一个前端R模块上，它会计算Hash值，Hash会随机落在任意一个C上，没有谁特殊。这样一切都是线性的，X-Brick的增减会线性地导致性能增减。

2.6.5 应用场景

闪存价格现阶段还是比较昂贵的，尤其是企业级应用使用的eMLC或SLC，所以全闪存阵列XtremIO并不能取代大容量的存储阵列SAN。那它跟哪种应用场景比较般配呢？想想就知道了，闪存的优势就是延迟低、性能高，所以适用于容量要求不高，但是要求延迟低、高IOPS的应用，比如VDI（虚拟桌面基础架构，就是虚拟机）、数据库、SAP等企业应用。

数据库是非常受益的，为什么？首先是性能高，其次就是复制几乎不占空间，所以用户可以很方便、快速地为数据创建多个副本。

已经有人在一个X-Brick上运行了2500~3500个VDI虚拟机，而延迟在1ms以内。虚拟机很多数据也是重复的，毕竟每个系统的文件都差不多，所以去重也能发挥很大作用。

企业应用领域也有人使用XIO加速了关键应用。

总之，只要容量足够，那你的应用用起来肯定比以前快多了！

看完了整个全闪存阵列XIO的技术揭秘，我们发现其实XIO的核心还是在软件，因为硬件都是标准件，都是X86服务器、SAS接口的SSD。AFA到底有什么独特的地方呢？

相比SSD，它没有垃圾回收、Wear Leveling、Read Disturb等传统SSD的功能，因为这些都在SSD里面由主控搞定了。

相比传统阵列，它的特色是去重和RAID 6每次写到新的地址的功能。

以前可能你也不知道全闪存阵列到底是怎么弄的，看完了这一节，相信你 already 不觉得它神秘了。甚至可以这样看：U盘是一两个闪存芯片和控制器封装，SSD是很多U盘的阵列，全闪存阵列是很多SSD的阵列，只不过U盘是最差的闪存，SSD好一点，AFA用得更好。但是，每升一级，就是一次质变，应用场景也各不相同，软硬件架构要重新设计。

2.7 带计算功能的固态硬盘

黑科技年年有，今年尤其多。比如Google的机器学习处理器TPU 2.0，性能直接震惊了深度学习界扛把子NVIDIA。本来GPU只是耗电厉害，性能在通用方面还能称霸，没想到TPU来了之后，一下子GPU性能被比下去了，功耗还是TPU的好几倍。这也从一个侧面告诉我们，专用ASIC和FPGA等可定制逻辑的深度学习计算平台才是未来的发展方向，因为它们有很大的潜力可以挖掘，通过架构的不断创新，未来能达到的性能会很高。

我们都知道，现在是一个数据爆炸的时代，一方面手机、平板等各种移动设备在产生大量用户数据；另一方面遍布全世界的各种传感器，比如摄像头、无人驾驶汽车的各种探头等每天都在产生海量视频数据，视频和图像才是信息时代数据的大头。举个例子，一辆无人驾驶汽车的传感器、激光雷达、毫米波雷达等1天就会产生64TB的数据！

支撑起这一巨大数据网络的根基是IT基础设施，主要包括网络、计算和存储三大部分。

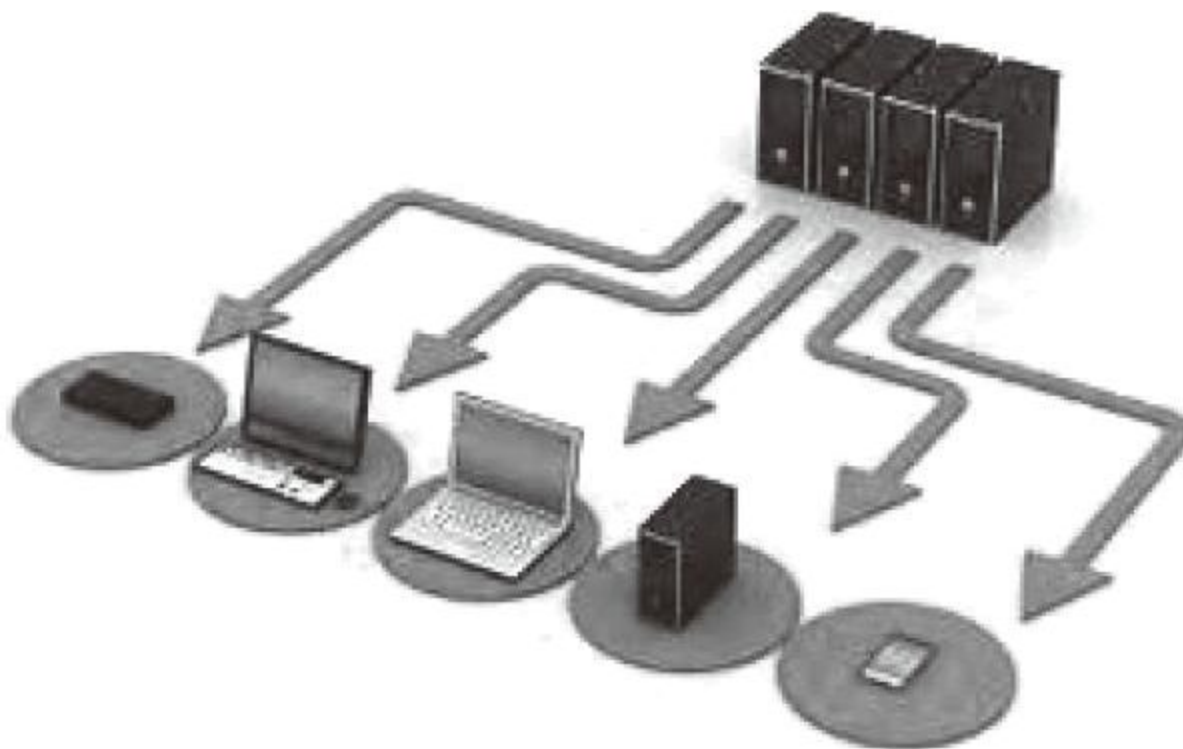


图2-34 IT基础架构

IT基础架构的功能就跟加工贸易差不多，网络是数据的搬运工，计算是数据的加工商，存储就是数据的窝。现在，网络已经非常高速了，家里百兆宽带都很常见，手机用4G也能看看小电影。以前，存储是个麻烦事，想想当年360开机助手每次提醒的电脑开机时间有多久，机械硬盘马达轰隆隆转个不停，读数据还慢悠悠。

但是，自从有了固态硬盘之后，存储就不是事儿了，最新的PCIe 3.0x8 SSD，读写带宽能达到4GB/s以上！一方面存储进步快，而另一方面CPU又受摩尔定律失效限制，工艺进展缓慢，所以，计算成了瓶颈，尤其是在图像和视频处理、深度学习等方面。海量数据能够从PCIe SSD高速读写，但就是CPU处理不过来。

那么，把存储和计算结合起来是不是就可以解决这个痛点呢？位于中国上海的一家公司——方一信息科技推出了一款黑科技产品：带FPGA的SSD——CFS（Computing Flash System，计算闪存系统）。它采用PCIe 3.0x8高速接口，性能可达5GB/s。SSD提供高速数据存储，FPGA能提供计算加速，这样数据从SSD出来就由FPGA顺带算好，释放了CPU。一切回归原位，CPU做控制，FPGA做计算，SSD做存储。

那么，这个东西有什么用处呢？它的优势主要体现在海量数据高速存储和人工智能计算方面。想一想就会有很多场景，比如无人驾驶汽车，目前一般的无人驾驶汽车配备了毫米波雷达、激光雷达、高速摄像头等各类传感器。每秒会产生1GB数据，要分析这么多数据需要强大的计算能力。很多无人驾驶汽车还在使用GPU进行计算。目前市场上在卖的一个CPU+GPU计算盒，功耗能达到5000W，对于汽车来说，这个小火罐的散热会带来很大的安全风险，同时也很耗电。但是，如果换用了FPGA方案，功耗就可以降下来，根据无人驾驶的应用场景对算法进行优化之后，计算性能也能满足需求。例如，奥迪公司的无人驾驶汽车就采用了FPGA计算平台。这些传感器产生的数据目前都是丢掉，非常可惜，未来商用之后，不管是政府还是厂商都有存储宝贵的行驶数据并备份到云端的需求。这些数据对于完善无人驾驶、分析车祸现场都非常有用。要保存这些数据，只有PCIe SSD才能达到1GB/s以上的写速度。所以，FPGA SSD一方面能够快速存储行驶数据，一方面又可以提供FPGA进行数据分析，完美满足无人驾驶的计算与存储需求。

自从人工智能开始新一轮的热潮之后，很多公司都开始用FPGA做人工智能计算，用了CFS，就可以直接用FPGA里的人工智能硬件算法对SSD内部的海量数据进行高速分析，最后把分析结果发送给主机。

可能有人要问，FPGA和闪存芯片中国还不能国产。其实，FPGA中国已经有很多国产厂商在做，并达到主流性能；而闪存芯片长江存储在2018年就有希望量产供货了。

第3章 SSD存储介质：闪存

读者君知道，你一边吃着地铁口刚买的杂粮煎饼，一边啃读的这本书是负责SSDFans微信公众号的几位作者倾力合著的，其中阿呆负责撰写的就是闪存这一章。有一个名人说过，书能传神，当你看书的时候，阿呆也闻到了杂粮煎饼那浓浓的葱香味儿。

3.1 闪存物理结构

3.1.1 闪存器件原理

前文已经讲过了固态硬盘的发展史，曾经的固态硬盘有过RAM等介质，但是目前绝大多数固态硬盘都是以闪存芯片为存储介质的。**DRAM**固态硬盘我们见得少，主要应用于特殊的场合。1978年诞生的世界上第一块固态硬盘就是基于**DRAM**的。但由于保存在**DRAM**中的数据有掉电易失性，当然还有成本因素，所以现在的固态硬盘一般都不采用**DRAM**，而是使用闪存作为存储介质，并且是**NAND**闪存。固态硬盘的工作原理很多也都是基于闪存特性的。比如，闪存在写之前必须先擦除，不能覆盖写，于是固态硬盘才需要垃圾回收（**Garbage Collection**，或者叫**Recycle**）；闪存每个块（**Block**）擦写次数达到一定值后，这个块要么变成坏块，要么存储上面的数据不可靠，所以固态硬盘固件必须做磨损平衡，让数据平均写在所有块上，而不是盯着几个块拼命写（不然很快固态硬盘就报废了）。还有很多类似的例子，固态硬盘内部很多算法都是在为闪存服务的。所以，欲攻固态硬盘，闪存首当其冲。

闪存是一种非易失性存储器，也就是说，掉电了数据也不会丢失。闪存基本存储单元（**Cell**）是一种类**NMOS**的双层浮栅（**Floating Gate**）**MOS**管，如图3-1所示。

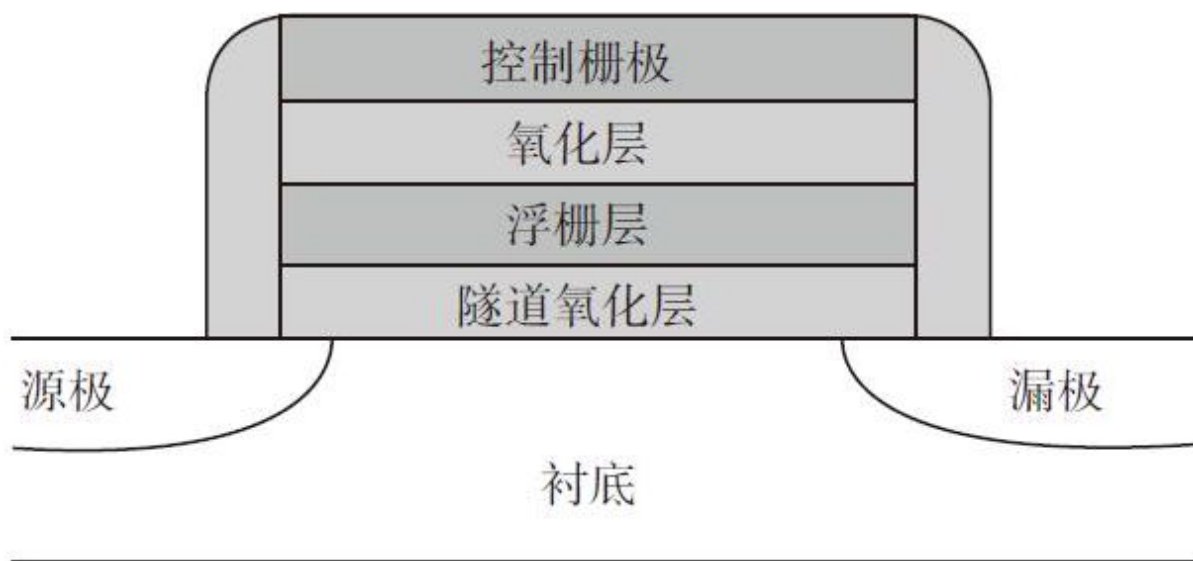


图3-1 浮栅晶体管结构

在源极（Source）和漏极（Drain）之间电流单向传导的半导体上形成存储电子的浮栅，浮栅上下被绝缘层包围，存储在里面的电子不会因为掉电而消失，所以闪存是非易失性存储器。

写操作是在控制极加正电压，使电子通过绝缘层进入浮栅极。擦除操作正好相反，是在衬底加正电压，把电子从浮栅极中吸出来，如图3-2所示。

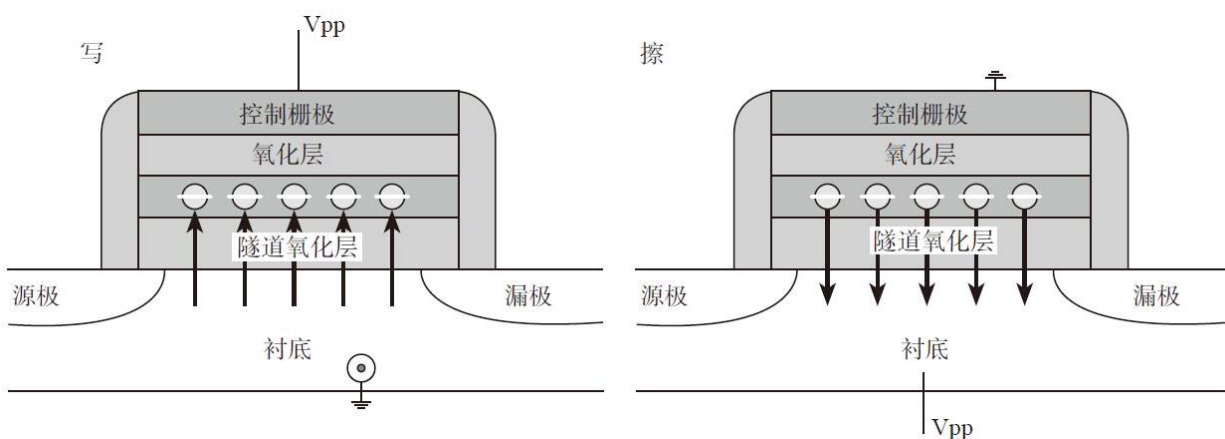


图3-2 左：写原理；右：擦除原理

在2014年的闪存峰会上，浮栅晶体管的发明人施敏（Dr.Simon Sze）被授予终身成就奖，以表彰他发明了浮栅极晶体管。据说，浮栅极晶体管的发明灵感是这样来的：某天，施敏和搭档Dawon Kahng在公司的食堂一起吃午餐，饭后甜点是奶酪蛋糕。看着夹心蛋糕，他们在想，如果在MOS场效应管中间加个东西，会怎样呢？于是，浮栅晶体管横空出世。截至2014年的某个时间点，据统计，全世界生产的浮栅晶体管数目达1074344929692350000000。

这个数字还在继续增长着。阿呆觉得终身成就奖不够，施敏应该获得诺贝尔奖，毕竟机械硬盘机理——巨磁阻效应的发现人已经获得了诺贝尔奖。

获奖后，施敏在庆功宴上为自己点了一份奶酪蛋糕。

3.1.2 SLC、MLC和TLC

一个存储单元存储1bit数据的闪存，我们叫它为SLC（Single Level Cell），存储2bit数据的闪存为MLC（Multiple Level Cell），存储3bit数据的闪存为TLC（Triple Level Cell），如表3-1所示。现在已经有厂商在研发QLC，即一个存储单元存储4bit数据，本书不做介绍。

表3-1 SLC、MLC、TLC原理

SLC	MLC		TLC			SLC	MLC		TLC		
0	0	0	0	0	0	1	1	0	1	0	0
			0	0	1				1	0	1
	0	1	0	1	0		1	1	1	1	0
			0	1	1				1	1	1

对SLC来说，一个存储单元存储两种状态，浮栅极里面的电子多于某个参考值的时候，我们把它采样为0，否则就判为1。

图3-3是闪存芯片里面存储单元的阈值电压分布函数，横轴是阈值电压，纵轴是存储单元数量。其实在0或1的时候，并非所有的存储单元都是同样的阈值电压，而是以这个电压为中心的一个分布。读的时候采样电压值落在1范围里面，就认为是1；落在0范围里面，就认为是0。

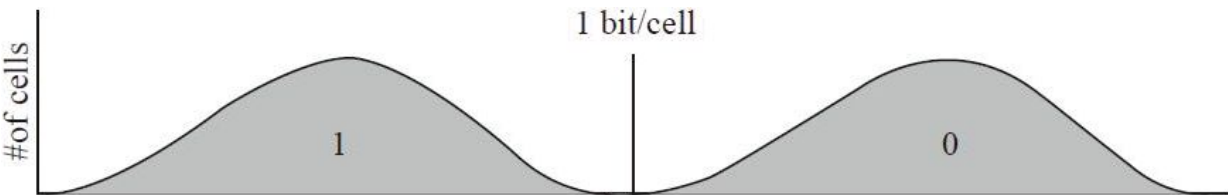


图3-3 SLC电压分布

擦除之后，闪存读出来的值为1，充过电之后，就是0。所以，如果需要写1，就什么都不用干；写0，就需要充电到0。

对MLC来说，如果一个存储单元存储4个状态，那么它只能存储2bit的数据，如图3-4所示。通俗来说就是把浮栅极里面的电子个数进行一个划分，比如低于10个电子判为0；11~20个电子判为1；21~30个电子判为2；多于30个电子判为3。

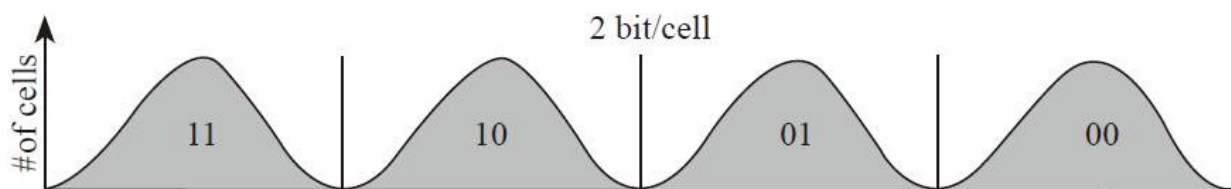


图3-4 MLC电压分布

依此类推，TLC若是一个存储单元有8个状态，那么它可以存储3bit的数据，它在MLC的基础上对浮栅极里面的电子数又进一步进行了划分，如图3-5所示。

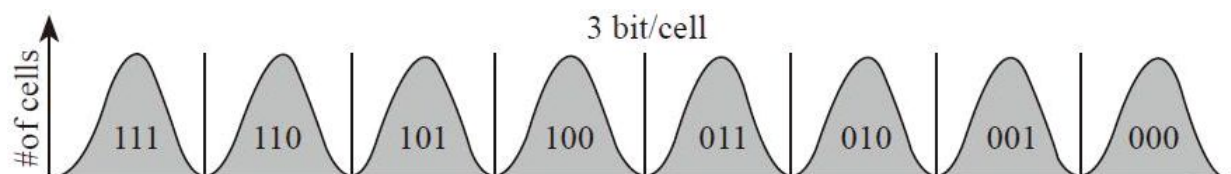


图3-5 TLC电压分布

同样面积的一个存储单元，SLC、MLC和TLC分别可以存储1bit、2bit、3bit的数据，所以在同样面积的DIE上，闪存容量依次变大。

但同时，一个存储单元电子划分得越多，那么在写入的时候，控制进入浮栅极的电子个数就要越精细，所以写耗费的时间就越长；同样的，读的时候，需要尝试用不同的参考电压去读取，一定程度上加长了读取时间。所以我们会看到在性能上，TLC不如MLC，MLC不如SLC。

如表3-2所示是SLC、MLC和TLC在性能和寿命（Endurance）上的一个直观对比（不同制程和不同厂家的闪存，参数不尽相同，数据仅供参考）。

表3-2 SLC、MLC、TLC参数比较

闪存类型	SLC	MLC	TLC	闪存类型	SLC	MLC	TLC
每单元比特数	1	2	3	写时间 (μs)	约 300	约 600	约 900
擦写次数	约 10 万次	约 5000 次	约 1000 次	擦除时间 (μs)	约 1500	约 3000	约 4500
读时间 (μs)	约 25	约 50	约 75				

3D TLC逐渐成为主流。同时，QLC也马上就要量产了，每个存储单元存储4bit数据，比TLC还要慢，还要不可靠。之前怀疑TLC可靠性的

人们，怎么看QLC？

3.1.3 闪存芯片架构

闪存芯片就是由成千上万这样的存储单元按照一定的组织结构组成的。

图3-6所示是一个闪存块（Block）的组织架构。一个Wordline对应着一个或若干个Page，具体是多少取决于SLC、MLC或者TLC。对SLC来说，一个Wordline对应一个Page；MLC则对应2个Page，这两个Page是一对（Lower Page和Upper Page）；TLC对应3个Page（Lower Page、Upper Page和Extra Page，不同闪存厂家叫法不一样）。一个Page有多大，那么Wordline上面就有多少个存储单元，就有多少个Bitline。一个Block当中的所有这些存储单元都是共用一个衬底的。

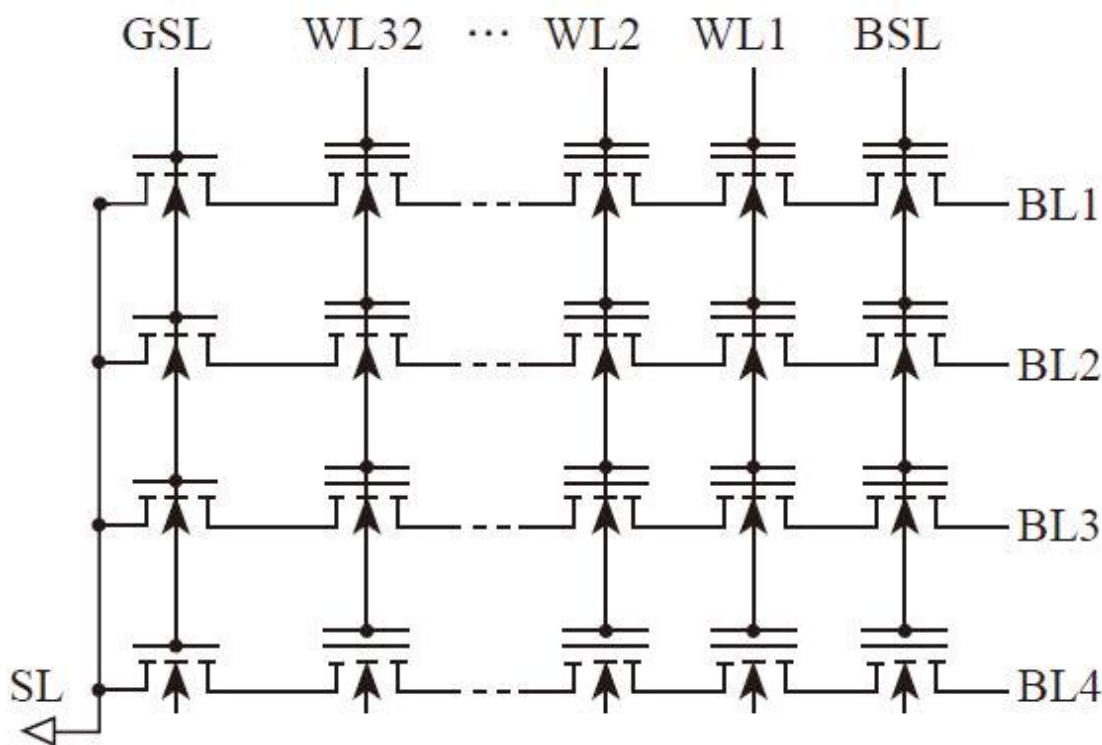


图3-6 闪存Block组织架构

这里没有考虑奇/偶Bitline，否则一个Wordline上的Page数量在此基础上要翻倍。

一个闪存内部的存储组织结构如图3-7所示：一个闪存芯片有若干个DIE（或者叫LUN），每个DIE有若干个Plane，每个Plane有若干个Block，每个Block有若干个Page，每个Page对应着一个Wordline，Wordline由成千上万个存储单元构成。

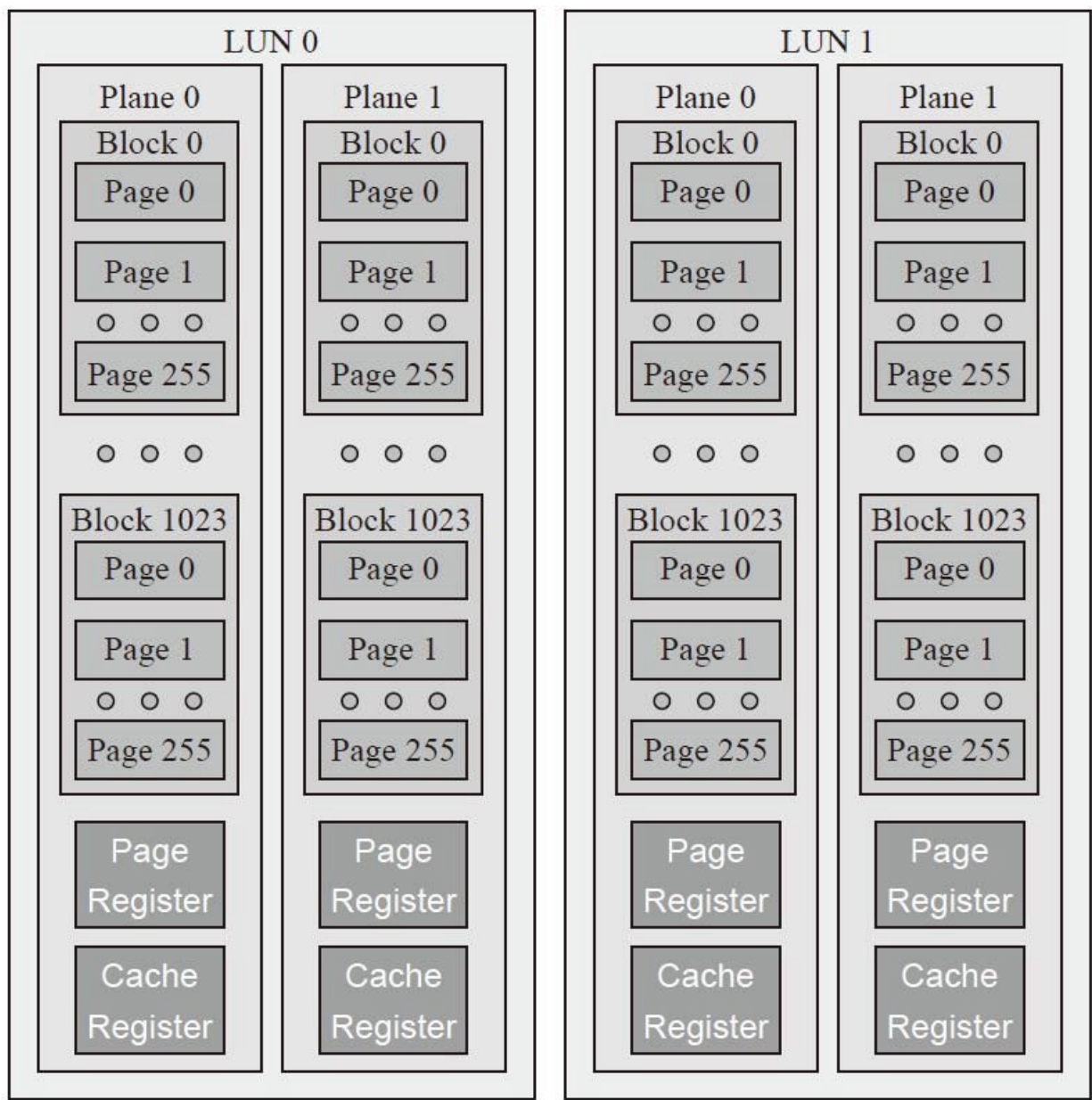


图3-7 闪存内部组织架构

DIE/LUN是接收和执行闪存命令的基本单元。如图3-7所示，LUN0和LUN1可以同时接收和执行不同的命令（但还是有一定限制的，不同厂家的闪存限制不同）。但在一个LUN当中，一次只能独立

执行一个命令，你不能对其中某个Page写的同时，又对其他Page进行读访问。

一个LUN又分为若干个Plane，市面上常见的是1个或者2个Plane，现在也有4个Plane的闪存了。每个Plane都有自己独立的Cache Register和Page Register，其大小等于一个Page的大小。固态硬盘主控在写某个Page的时候，先把数据从主控传输到该Page所对应Plane的Cache Register当中，然后再把整个Cache Register当中的数据写到闪存阵列；读的时候则相反，先把这个Page的数据从闪存介质读取到Cache Register，然后再按需传给主控。这里按需是什么意思？就是我们读取数据的时候，没有必要把整个Page的数据都传给主控，而是按需选择数据传输。但要记住，无论是从闪存介质读数据到Cache Register，还是把Cache Register的数据写入闪存介质，都以Page为单位，如图3-8所示（不过有些闪存支持partial program/read，这不在讨论之列）。

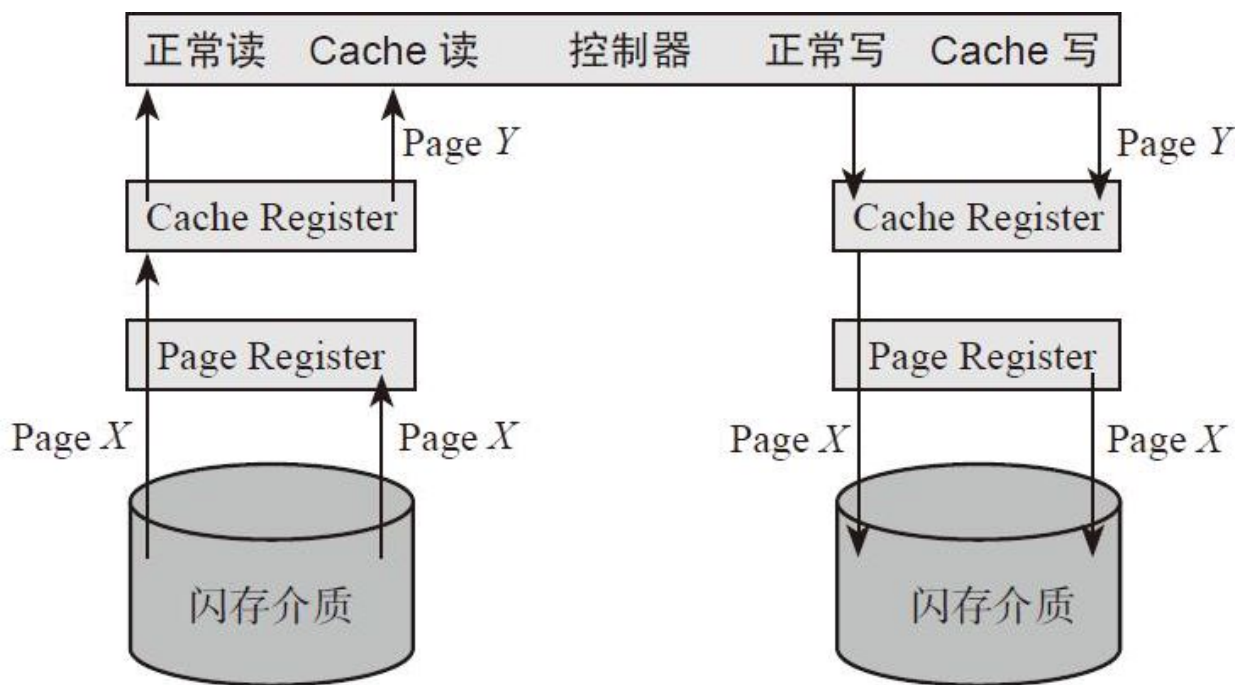


图3-8 Page缓存的用法

为什么需要Cache Register和Page Register两个缓存？主要目的是优化闪存的访问速度。闪存支持Cache读、写操作，如图3-8所示。Cache读支持在传输前一个Page数据给主控的时候（Cache Register→主控），可以从闪存介质读取下一个主控需要读的Page的数据到Page Register（闪存介质→Page Register），这样数据在闪存总线传输的时间

就可以隐藏在读闪存介质的时间里（或者相反，取决于哪个时间更长）；Cache Program也是如此，它支持闪存写前一个Page数据的同时（Page Register → 闪存介质），传输下一个要写的数据到Cache Register（主控 → Cache Register），这样数据在闪存总线传输可以隐藏在前一个Page的写时间里。

当然，有两个Register的闪存也支持正常的读写模式，这时候，用户可以把Cache Register和Page Register看成是一个缓存。

我们通常所说的闪存读写时间，并不包含数据从闪存到主控之间的数据传输时间，也不包括数据在Cache Register和Page Register之间的传输时间。闪存写入时间是指一个Page的数据从Page Register当中写入闪存介质的时间，闪存读取时间是指一个Page的数据从闪存介质读取到Page Register的时间。

闪存一般都支持Multi-Plane（或者Dual-Plane）操作。那么什么是Multi-Plane操作呢？对写来说，主控先把数据写入第一个Plane的Cache Register当中，数据保持在那里，并不立即写入闪存介质，等主控把同一个LUN上的另外一个或者几个Plane上的数据传输到相应的Cache Register当中，再统一写入闪存介质。假设写入一个Page的时间为1.5ms，传输一个Page的时间为50μs：如果按原始的Single Plane操作，写两个Page需要至少 $(1.5\text{ms} + 50\mu\text{s}) \times 2$ ；但如果按照Dual-Plane操作，由于隐藏了一个Page的写入时间，写入两个Page只要 $1.5\text{ms} + 50 \times 2\mu\text{s}$ ，缩减了几乎一半的时间，写入速度几乎翻番。对读来说，使用Dual-Plane操作，两个不同Plane上的Page数据会在一个闪存读取时间加载到各自的Cache Register当中，这样用一个读取时间读取到两个Page的数据，读取速度加快。假设读取时间和数据传输时间相当，都是50μs，Single Plane读取传输两个Page需要 $50\mu\text{s} \times 4 = 200\mu\text{s}$ ，Dual-Plane则需要 $50\mu\text{s} \times 2 + 50\mu\text{s} = 150\mu\text{s}$ ，时间为前者的75%，读取速度也有很大的提升。

闪存的擦除是以Block为单位的。为什么呢？那是因为在组织结构上，一个Block当中的所有存储单元是共用一个衬底的（Substrate）。当你对某衬底施加强电压，那么上面所有浮栅极的电子都会被吸出来。每个闪存Block都有擦写次数的限制，这个最大擦写次数按SLC、MLC、TLC依次递减：SLC的擦写次数可达10万次，MLC一般为几千到几万次，TLC降到几百到几千次。随着闪存工艺的不断进步（现在已经进入1Xnm时代），闪存容量不断加大，但性能与可靠性却在变差。

要克服闪存的这些不利因素，固态硬盘固件算法需要面对更多、更大的挑战。

3.1.4 读、写、擦原理

闪存的基本操作是读、写、擦。下面来具体介绍，各种参数仅供参考（不同闪存参数不同）。

1.擦除

如图3-9所示，擦除前，浮栅上有可能有电子，**Pwell**加20V电压，经过足够时间后，由于量子隧道效应，电子从浮栅到沟道里面，完成一个**Block**的擦除，阈值电压都变成了 $-V_T$ ，状态为“1”。一个**LUN**上的**MOS**管共用一个**Pwell**，但是其他不用擦除的**Block**的栅极电压是悬空，不会有隧道效应。

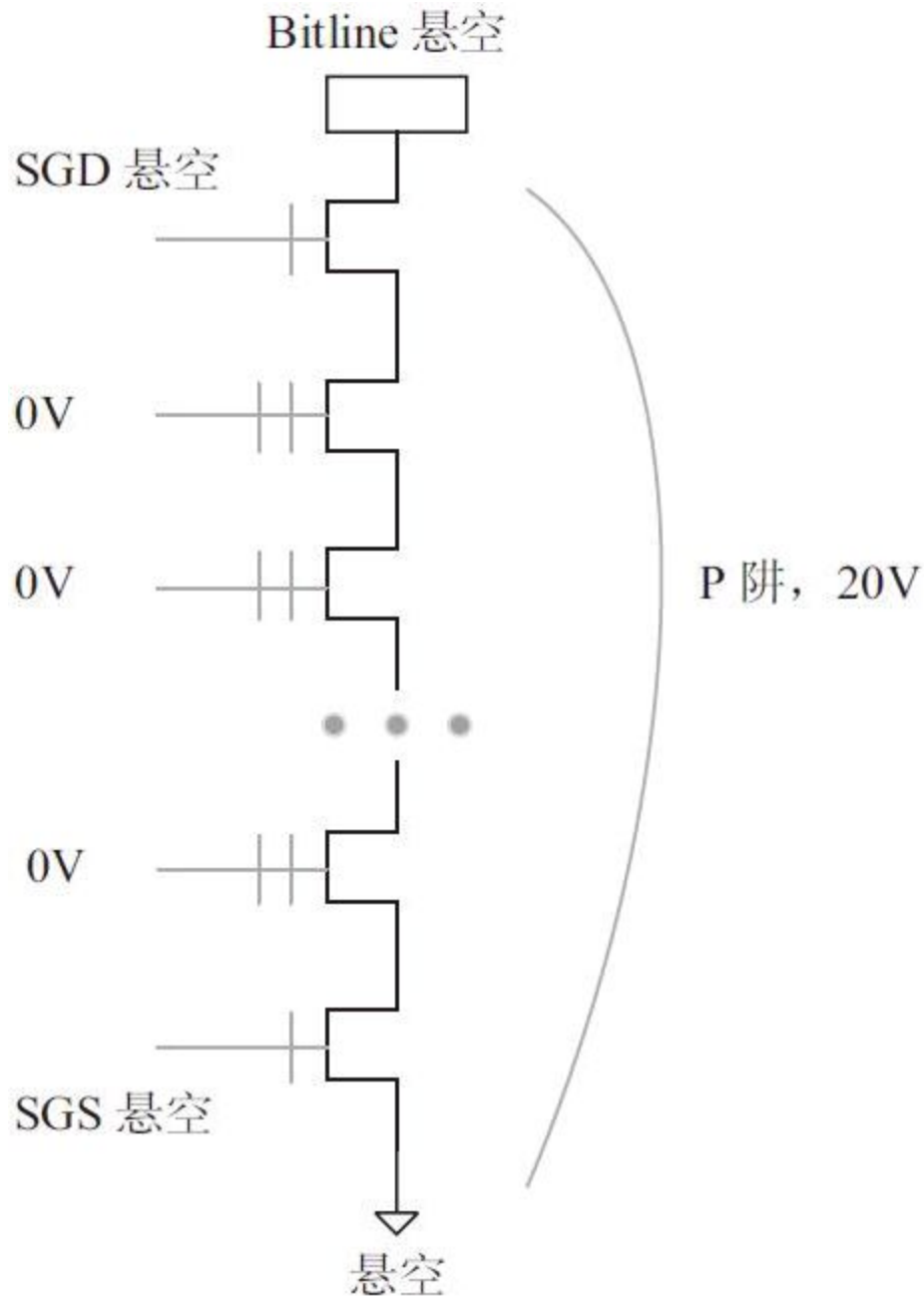


图3-9 擦除操作电压示例

2.写

如图3-10所示，擦除后所有的单元阈值电压为 $-V_T$ ，写电压如下：要写的单元Wordline为高电压，Bitline=0V；由于量子隧道效应，电子从沟道到浮栅，成为“0”。不写的单元Bitline为2V，在沟道里的效应阻碍了量子隧道效应发生。

3.读

不读的Wordline=5V，管子保持导通；要读的单元Wordline=0V， $-V_T$ 的管子导通，Bitline端的传感器能够检测到，所以读到“1”，而经过写的+VT的管子不导通，传感器读为“0”。

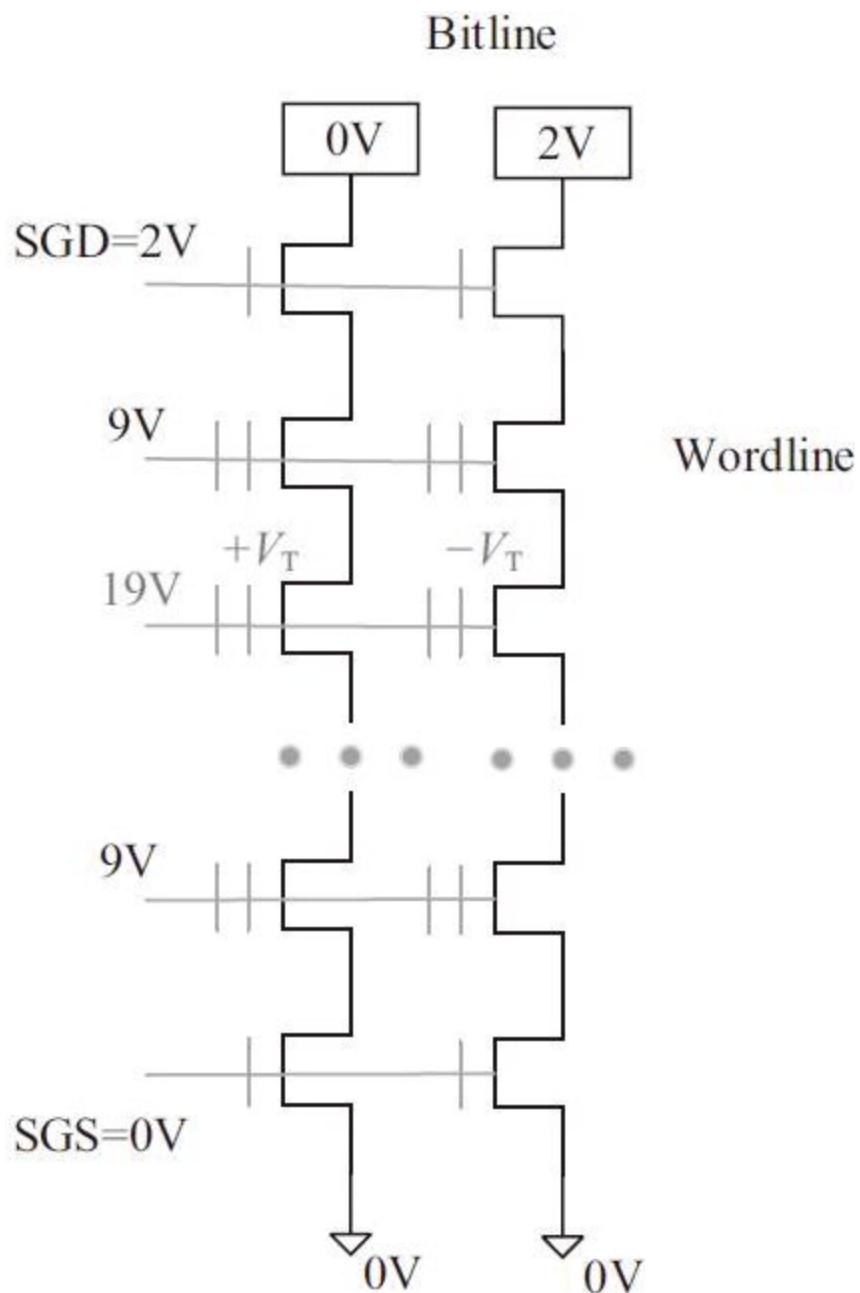


图3-10 写入操作电压示例

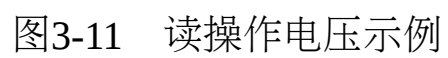


图3-11 读操作电压示例

3.1.5 三维闪存

因为集成密度高、单位比特成本低和可靠性高等众多优点，闪存占据了手机、平板、固态硬盘等绝大部分的非易失性存储市场。可是因为技术上的限制，这些优势越来越难以维持下去。

即使2次曝光技术（Double Patterning Technology）和4次曝光技术（Quadruple Patterning Technology）的引入提高了制造工艺，但随着一代又一代半导体制造技术的演进，二维平面单元尺寸逐渐减小，单元间的相互干扰却在逐渐增加。基于二维平面单元结构的尺寸缩小已经无法进一步降低比特成本了，即达到了技术上的瓶颈。

图3-12为过去十年的单元尺寸与单元相互干扰的变化趋势图。从上半部分可以看出，二维闪存单元尺寸不断下降，对应到下半部分就是单元间的相互干扰不断增加，但到了三维闪存后，尺寸居然又再次变大了，所以，单元间相互干扰大幅度减小。

本小节文字和图表是SSDFans作者帅师兄整理自论文H.Kim, S.J.Ahn, Y.G.Shin, K.Lee and E.Jung, “Evolution of NAND Flash Memory: From 2D to 3D as a Storage Market Leader,” 2017 IEEE International Memory Workshop (IMW), Monterey, CA, 2017。

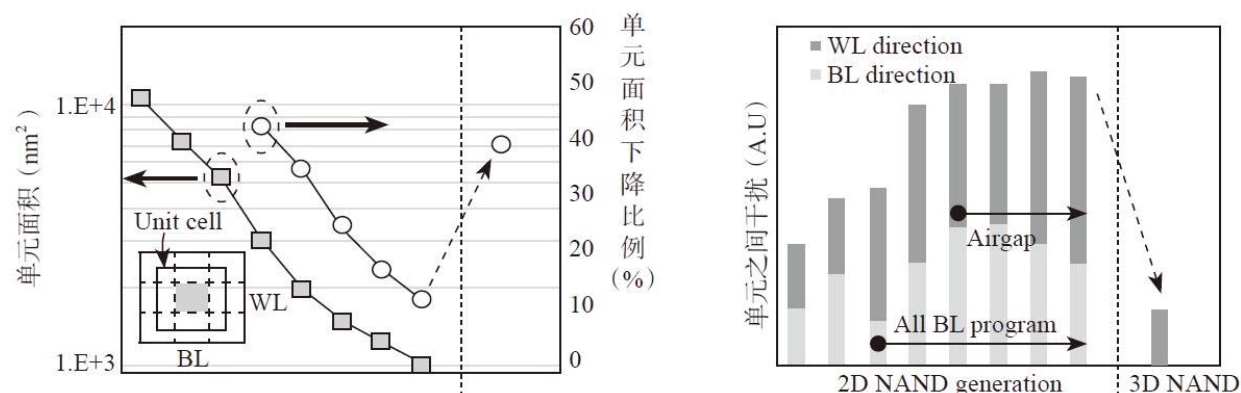


图3-12 过去十年的单元尺寸（左）与单元相互干扰（右）的变化趋势

为了克服二维平面单元结构的技术瓶颈，自2006年以来，各种三维闪存结构陆续被提出来。其中一种叫作TCAT，已经于2013年开始了规模化量产。三维闪存结构并不是利用传统的缩小单元的方法，而是

以提高堆叠栅极结构（WL）的数目来提高芯片的集成密度。平均来看，每一代三维闪存的堆叠栅极结构的数目都增长了40%，这意味着每一代单元尺寸减小了平均40%。因此，三维闪存快速地把二维闪存挤出了市场，应用三维闪存的固态硬盘也快速地替代了存储市场上的机械硬盘。如图3-13所示，根据iSuppli的调查，固态硬盘在闪存市场的份额从2013年到2017年，由23%增长到了43%。

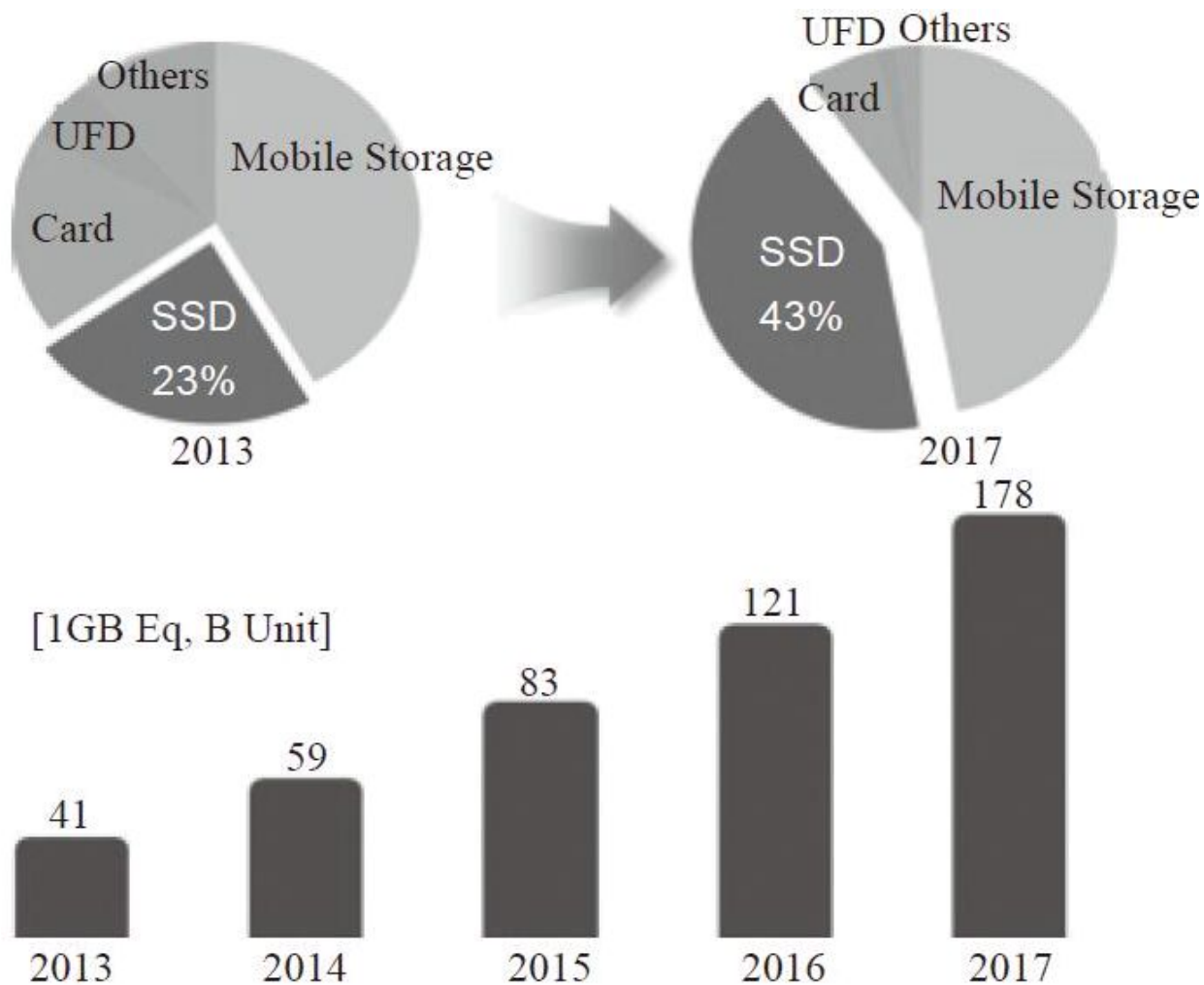


图3-13 固态硬盘在闪存市场的份额变化

图3-14是《Inside NAND Flash Memories》一书提供的某一类三维闪存的结构示意图，在这种三维闪存中，沟道是竖起来的，一层一层盖楼的是连接到栅极的Wordline。

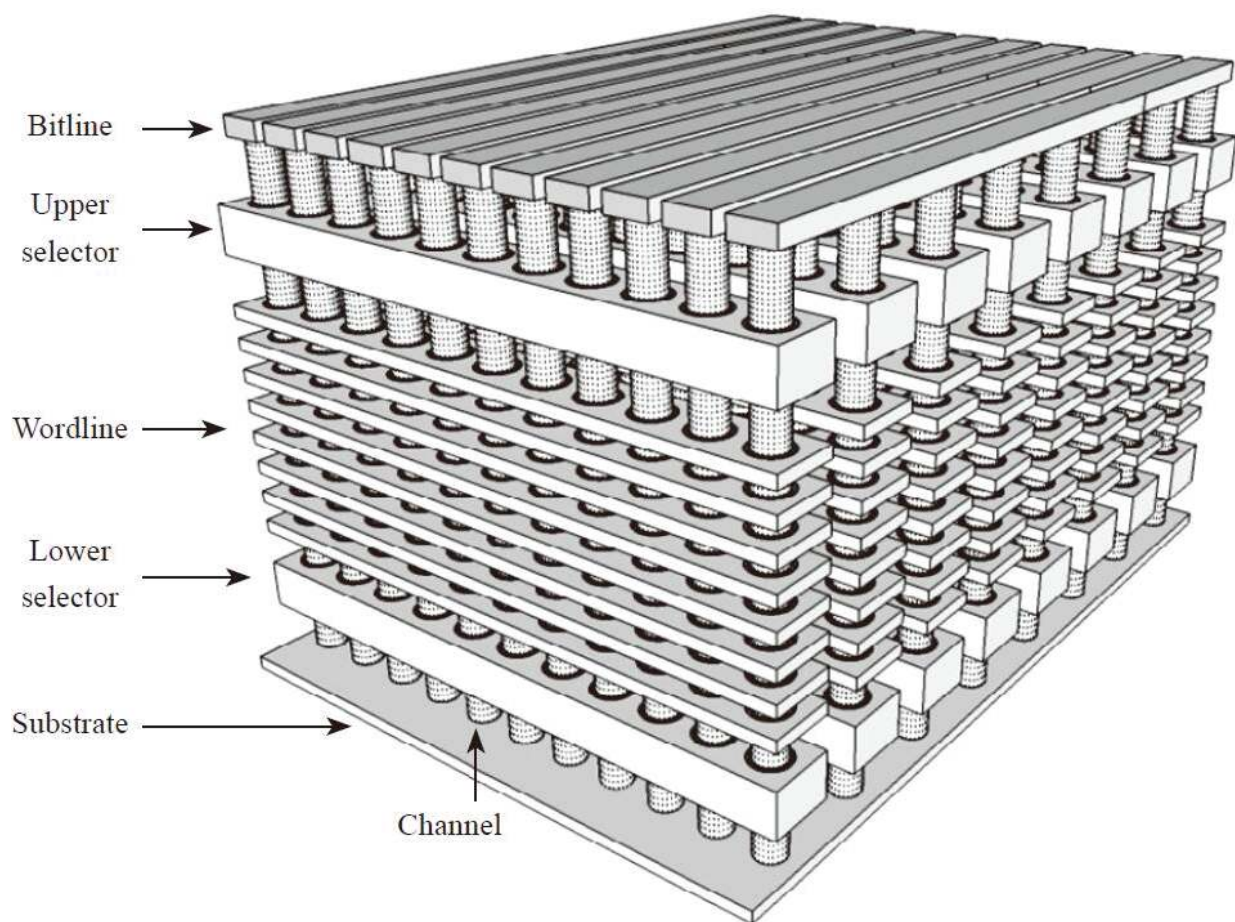


图3-14 三维闪存立体图

这里就不罗列历史上三维闪存的发展事件了，只把关键的两个事件点出来。2007年，BiCS（Bit Cost Scalable）技术（包含多堆叠栅极层结构）被提出；2009年，金属栅极三维闪存技术（Terabit Cell Array Transistor，TCAT）被提出来。BiCS和TCAT的具体对比如图3-15所示。其中，单元串的结构、单元堆叠的方式、编程/擦除窗口长短以及擦除方法等都是不同的。BiCS利用了多晶硅栅极，TCAT利用了金属栅极；BiCS的编程/擦除窗口比较窄，而TCAT的编程/擦除窗口就比较宽；BiCS的擦除方法是GIDL，而TCAT的擦除方法是群擦除方法（Bulk Erase）。二者的制造工艺流程也是不一样的。

与二维平面闪存相比，TCAT更加稳定、可靠而且性能水平更加优越。如图3-16所示，单元间相互干扰降低了84%，擦写寿命却提高了10倍以上，编程时间（ t_{PROG} ）也减少了一半，阈值电压 V_{th} 随着擦写增多带来的偏移也减小了67%。

自从24层堆叠的三维闪存可大规模生产以来，32层、48层及64层堆叠的三维闪存也接连投产。如图3-17所示，三维闪存的存储密度在每一代几乎都实现了翻倍。

不过三维闪存也面临下面两个挑战：

1) 堆叠栅极层数目增加带来的问题。正如前面所说，三维闪存通过增加堆叠栅极层的数目来提高比特密度，而且每一代堆叠栅极层数目都会增加30%~50%，这会带来许多困难，比如串电流的减小，高层与低层单元特征的差异性增大。

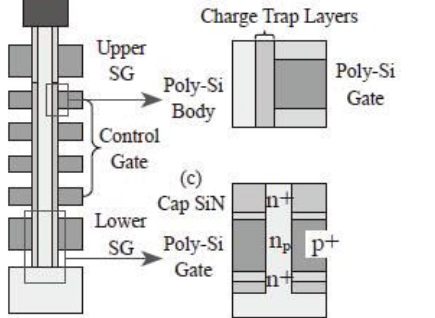
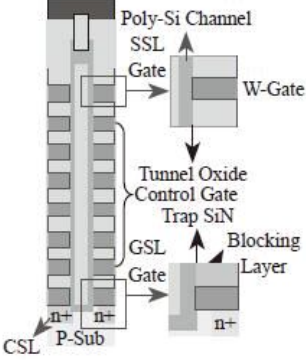
	BiCS	TCAT
单元串结构		
Cell Stack	SONOS (Poly-Si Gate)	TANOS (Metal Gate)
Word Line	Poly-Si (High R_s)	W (Low R_s)
Program/Erase 窗口	Narrow (SONOS)	Wide (TANOS)
擦除方法	GIDL	Bulk Erase
工艺	Poly (Gate)/Oxide depo. ↓ Ch. Hole etch ↓ Gate stack ↓ Ch. Poly depo.	Sin/Oxide depo. ↓ Ch. Hole etch ↓ Ch. Poly depo. ↓ SiN removal ↓ Gate stack depo. ↓ W (Gate) depo.

图3-15 BICS和TCAT工艺对比

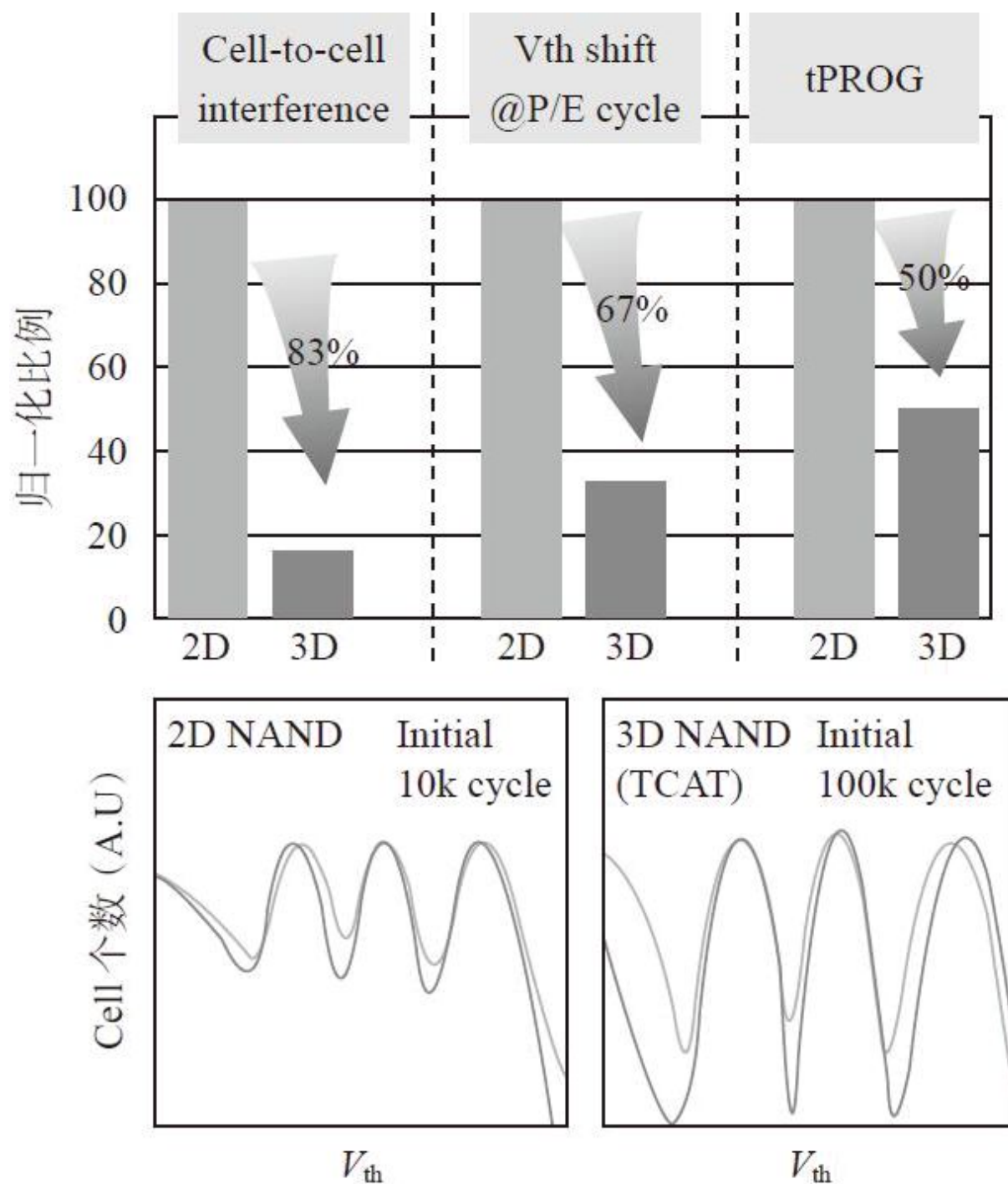


图3-16 二维闪存和TCAT三维闪存特性对比

具体地来讲，如图3-18所示，随着堆叠栅极层数目的增加，每个Block的Page数目不断增加。在读的过程中，对一个Block来说，累积的读取数目增加，导致读干扰会变严重。为了降低读干扰，需要降低读

参考电压 V_{read} ，这样就会导致串电流减小，使得提供给传感运放的信号更微弱。

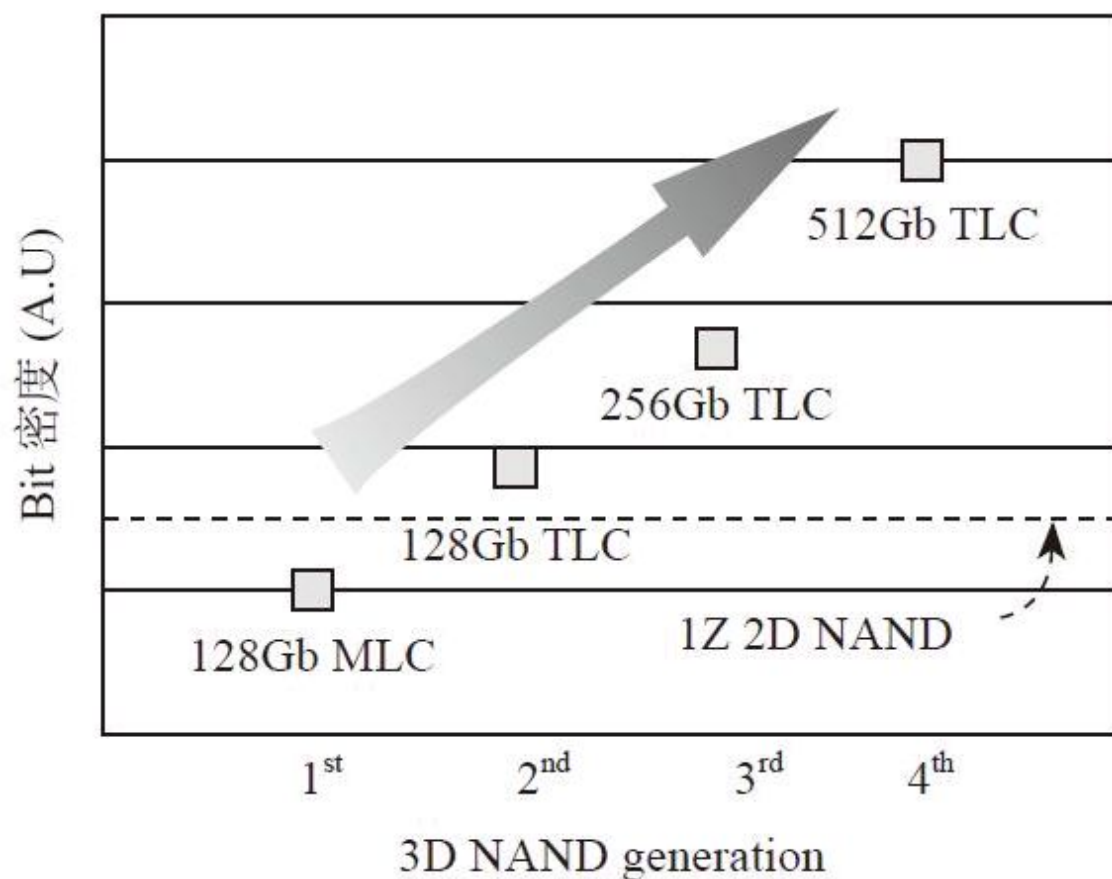


图3-17 三维闪存存储密度增长图

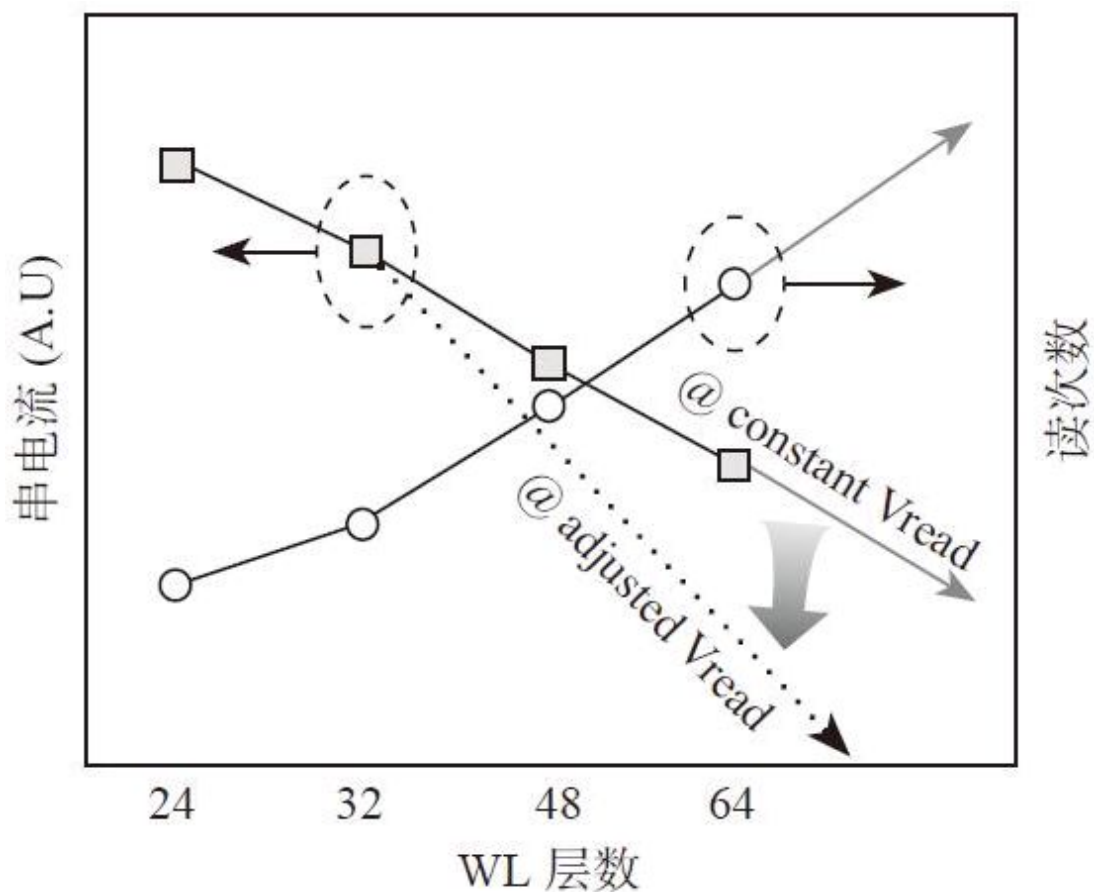


图3-18 层数越多，串电流变小，读次数增加

如图3-19所示，高层与低层之间的单元会存在差异。通道孔的尺寸大小和栅极厚度也存在差异，这些结构上的差异会带来编程/擦除速度的差异、单元间干扰的差异以及数据保存的差异等。

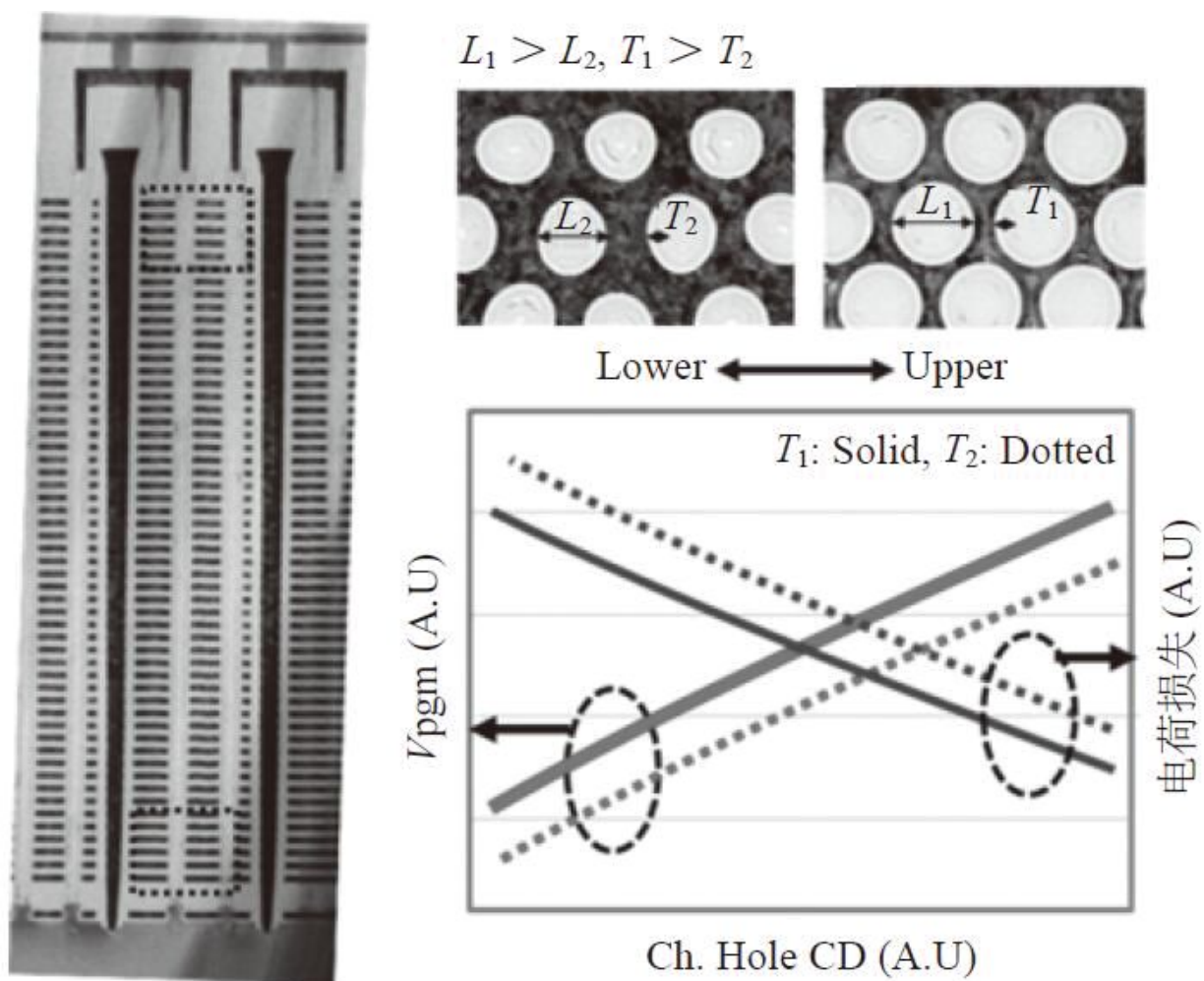


图3-19 高层和底层单元差异

底层单元的通道孔小，所以耦合率更高，擦写速度更快。但是，底层单元的栅极更薄，所以数据保存期更短。

2) **单元模具厚度减小带来的问题**。跟二维闪存类似，随着工艺一代一代迭代，最小尺寸也在不断减小，所以单元模具厚度不断减小，单元间的干扰也得到了增强。

3.1.6 Charge Trap型闪存

这里说的CT，不是医院里面的CT，而是闪存的一种技术——**Charge Trap**。最近流行一句话“生活不只是眼前的苟且，还有诗和远方”。套用一下，闪存不只有**Floating Gate**，还有**Charge Trap**。中文可以翻译成电阱，CT像个陷阱一样，把电荷困在里面存起来。

施敏和他的搭档在**MOSFET**中间加了一个浮栅极，创造了闪存的历史。此后有牛人在想，你中间加的是浮栅极，是导体，那我换个绝缘体怎么样？于是，CT技术的晶体管诞生了，如图3-20所示。

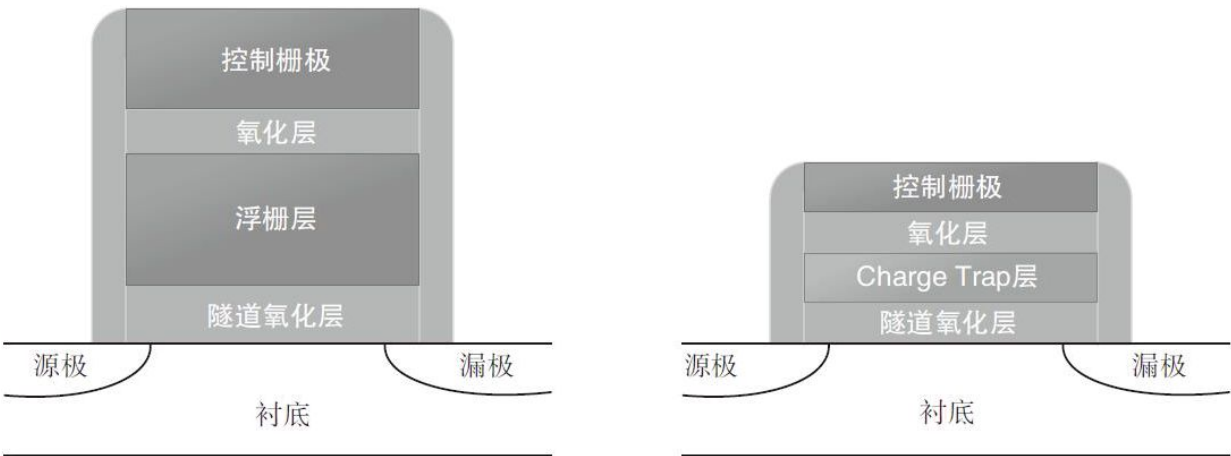


图3-20 浮栅晶体管与CT晶体管对比

CT与浮栅最大的不同是存储电荷的元素不同，后者是用导体存储电荷，而前者是用高电荷捕捉（**Trap**）密度的绝缘材料（一般为氮化硅，**Si3N4**）来存储电荷。CT的绝缘材料上面就像布了很多陷阱，电子一旦陷入其中，就难以逃脱，而浮栅是导体材料，电子可以在里面自由移动。有人是这样来形容两者区别的：浮栅就像水，电子可在里面自由移动；而CT就像是奶酪，电子在里面移动是非常困难的，如图3-21所示。

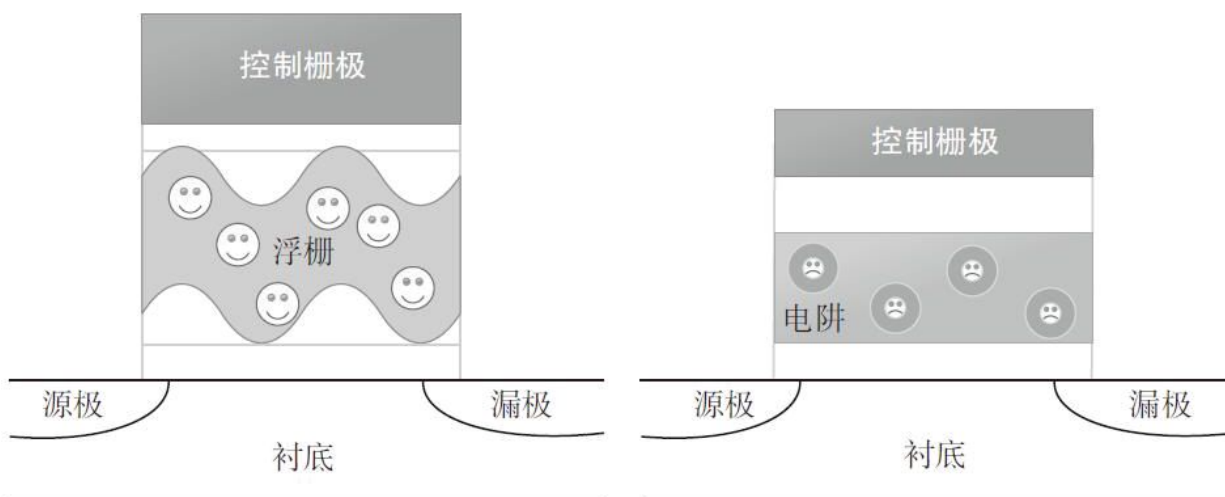


图3-21 浮栅像水，CT就像奶酪

为什么要强调电子不容易移动？

要知道，浮栅晶体管对浮栅极下面的绝缘层很敏感，该氧化物厚度变薄（制程不断减小导致的）或者老化（**Degradation**，擦写次数多了），浮栅极里面存储的电子进出变得容易。浮栅极里面的电子可以自由移动，因此对氧化层变得敏感。如果里面的电子本来就深陷其中，行动困难，即使绝缘层老化，电子还是不容易出来。因此，相对浮栅晶体管来说，CT的一个优势就是：对隧道氧化层不敏感，当厚度变薄或者擦除导致老化时，CT表示压力不大。

浮栅晶体管的浮栅极材料是导体，任何两个彼此绝缘且相隔很近的导体间都会构成一个电容器。因此，任何两个存储单元的浮栅极都构成一个电容器，一个浮栅极里面电荷的变化都会引起别的存储单元浮栅极电荷的变化。

一个浮栅极与其附近的浮栅极之间，都存在耦合电容（见图3-22），这个电容大小与彼此之间距离成反比：距离越短，电容越大，彼此影响越大（回想一下初中物理知识，平板电容器电容公式 $C = \epsilon S / 4\pi k d$ ，其中 d 就是平板之间距离）。随着闪存制程减小，存储单元之间影响越来越大。因此，存储单元间距也是影响制程继续往前的一个因素。CT对存储单元间距表示压力不大，因为存储电荷的是绝缘体，而非导体。

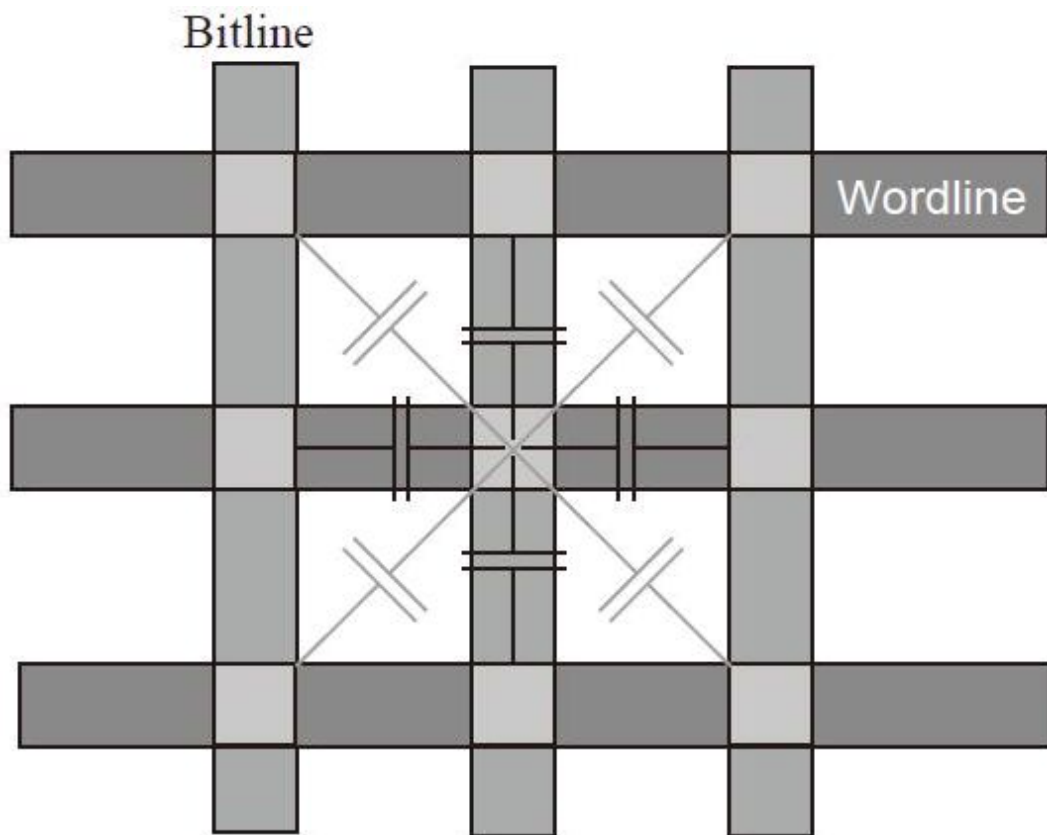


图3-22 浮栅晶体管之间耦合电容

与浮栅晶体管相比，CT擦写电压可以更小。为什么？

CT和浮栅晶体管对比图如图3-23所示，虽然这只是个示意图，但CT实际上确实比浮栅晶体管更矮：控制极到衬底之间的距离短。因此，要产生相同的隧道电场，加在控制极的电压可以更小（ $E=U/d$ ）。更小的写电压，使得隧道氧化层压力更小，因此绝缘氧化层损耗也慢。当然，还会更省电。

CT相比浮栅晶体管有很多优势，如上面提到的，对隧道氧化层要求不是那么苛刻；更小的存储单元间距；隧道氧化层磨损更慢；更节能；工艺实现容易；可以在更小的尺寸上实现。但是，CT也不能完胜。在Read Disturb和Data Retention方面，CT闪存就不如浮栅极闪存。

CT技术现在主要是应用在3D闪存上。如今除了美光使用浮栅极技术外，其他主流闪存商家都是用CT技术来制造3D闪存。

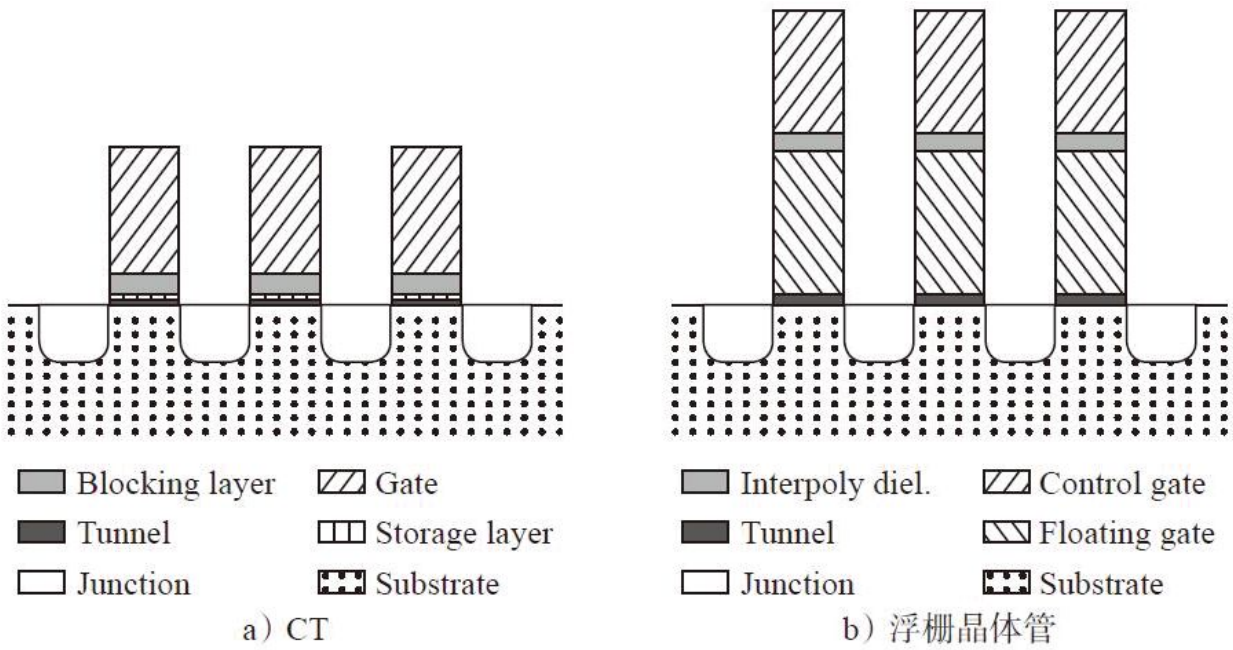


图3-23 CT和浮栅晶体管对比

3.1.7 3D XPoint

闪存用在固态硬盘上，使用SATA接口，要想更快可用SAS接口，甚至PCIe接口。其实最快的还是DRAM，可以支持字节级别的访问，但是DRAM上的数据如果不通电，马上就丢了。所以现代计算机同时使用DRAM和闪存存储数据。

最新的Intel Haswell-E/Broadwell处理器兼容的DDR4内存，读写速度可达61GB/s和46GB/s，而一个通道的PCIe SSD在理论上最高只能到1GB/s（PCIe 3.0）或者0.5GB/s（PCIe 2.0），一般SSD用4个通道，就是4GB/s或2GB/s。更慢的SATA理论上最高是600MB/s。

当然，机械硬盘就非常慢了，西部数据的VelociRaptor机械硬盘顺序读写速度分别为215MB/s和140MB/s。

所以，尽管PCIe SSD相比机械硬盘快20多倍，DDR4却是它的十几倍。最好是能找到和DRAM速度一样，数据却不会因掉电而丢失的存储器。江湖上有这么多自称有才的大侠：

- 忆阻器：ReRAM；
- 铁电存储器：FeRAM；
- 磁阻RAM：MRAM；
- 相变存储器：PRAM，PCM；
- 导电桥接RAM：cbRAM，又称可编程金属元存储器PMC；
- SONOS RAM：Silicon-Oxide-Nitride-Oxide-Silicon；
- 导电金属氧化物存储器：CMOx。

图3-24所示是各种新型存储器的容量成长之路，目前比较成熟的是相变存储器PCM——PRAM。

Intel的好友Micron一直以来在PCM上花了很多钱，2013年宣布实现了量产。Micron还把PRAM用到了诺基亚的Asha手机里面，1Gb的容量，写速度高达400MB/s。不过诺基亚手机的新东家微软说，Micron的PCM工艺还不够成熟，决定研发下一代PCM技术，降低功耗和成本，提高性能。

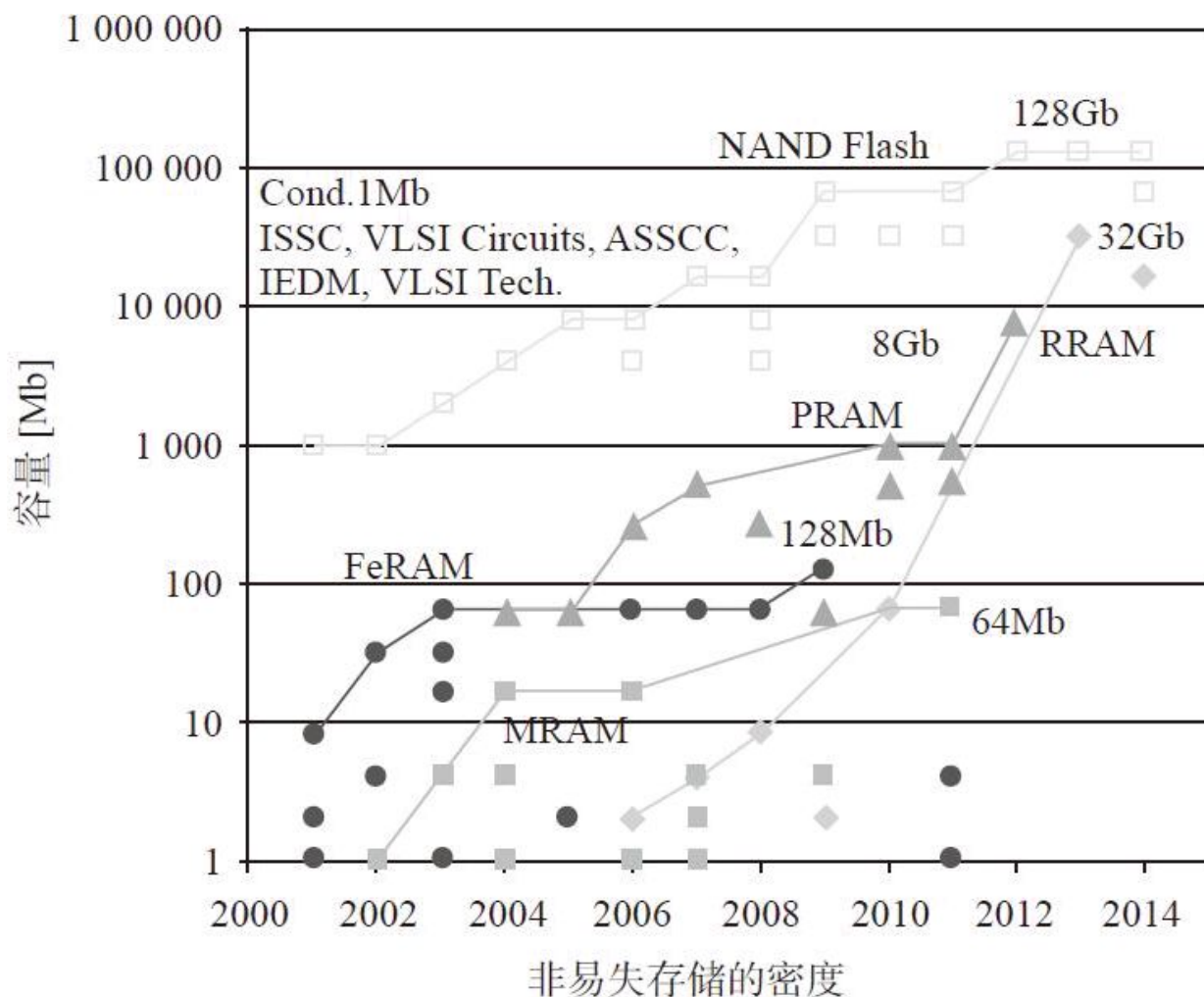


图3-24 新型存储器容量增长

所谓的相变存储器，就是在原子级别发生了相变，利用这个来存储数据。就像是玻璃经过相变成了晶体。这还是很好理解的，想想我们最常见的水，液体的时候形状不定，但是温度降低后，就发生相变，成为了固体——雪，雪就是晶体，有着稳定的晶体结构。如图3-25所示，左边是玻璃态，右边是晶体态，明显，晶体态更整齐。

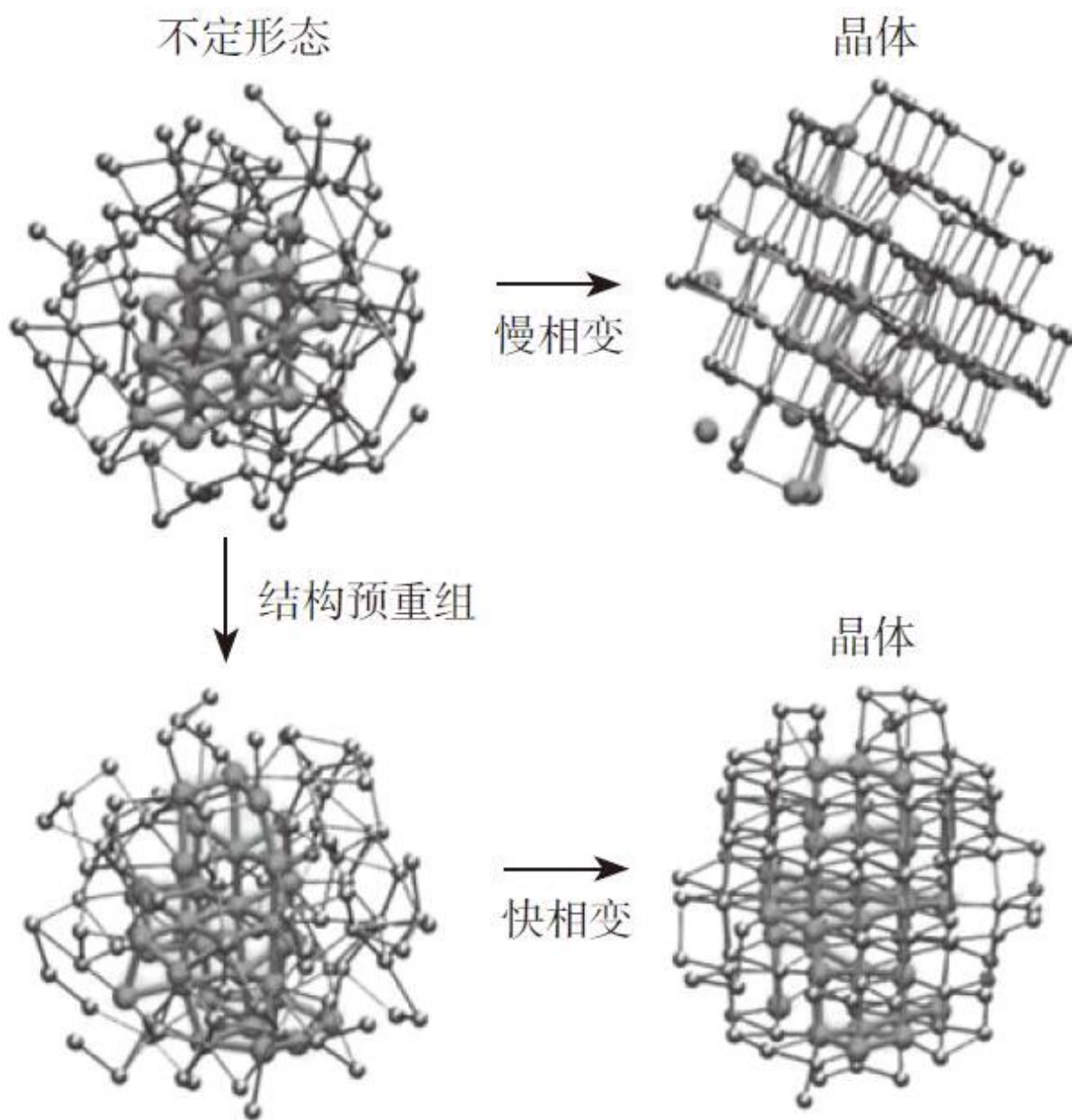


图3-25 相变晶体原理

物理原理讲完了，下面开始讲电气原理。不像DRAM里面有晶体管，PCM其实是通过一种微小的电阻作用使得玻璃融化，相变为晶体。技术日新月异，现在人类已经能高效地控制这种物理作用了，曾经写需要几微秒，读需要几纳秒，现在PCM已经能到皮秒的量级了，也就是纳秒的1000分之一，即 10^{-12} 秒。

来看看PCM和常见存储器的对比。表3-3中PCM的数据还在优化，最新的器件读写速度比表格里面快多了，里面的速度不是总线数据传

输速度，而是存储介质的读写速度。这个表格的数据比较旧，主要还是对存储器在功耗、寿命、功能等方面进行比较。可以看出，PCM的特点：

- 掉电数据不丢失；
- 可以按照字节访问；
- 软件简单；
- 写之前不需要擦除操作；
- 功耗低，和闪存差不多；
- 读写速度快；
- 寿命远长于闪存。

表3-3 几种存储器特性对比

特性	PCM	EEPROM	NOR Flash	NAND Flash	DRAM
掉电数据不丢失	是	是	是	是	否
支持字节级访问	是	是	是	否	是
需要擦除	否	否	是	是	否
软件复杂性	简单	简单	一般	复杂	简单
功耗	低	低	低	低	高
写带宽	1 ~ 15MB/s	13 ~ 30KB/s	0.5 ~ 2MB/s	>10MB/s	>100MB/s
读延迟	50 ~ 100ns	200ns	70 ~ 100ns	15 ~ 50μs	20 ~ 80ns
写次数	100 万次	10 万 ~ 100 万次	10 万次	1000 ~ 10 万次	无限次

Intel开发的相变存储器使用了硫属化物（Chalcogenides），这类材料包含元素周期表中的氧/硫族元素。Numonyx的相变存储器使用一种含锗、锑、碲的合成材料（Ge2Sb2Te5），多被称为GST。现今大多数公司在研究和发展相变存储器时都使用GST或近似的相关合成材料。

如图3-26所示，GST材料随着温度的上升，会从最左边的无定形态转变为右边的规则晶体结构，而电阻率也不断下降。这还是很好理解的，越有规则，导电性能就越好，电阻越小。但是，降温的过程中电阻值却不是可逆的，是底下那条直线。有半导体经验的人马上就明白

了，我们要知道数字电路之所以能表示1和0，就是因为有双稳态，有两个不可逆的稳定状态。这种相变材料恰好有这种特性，所以就能用来表示1和0了，也就能存储数据了。

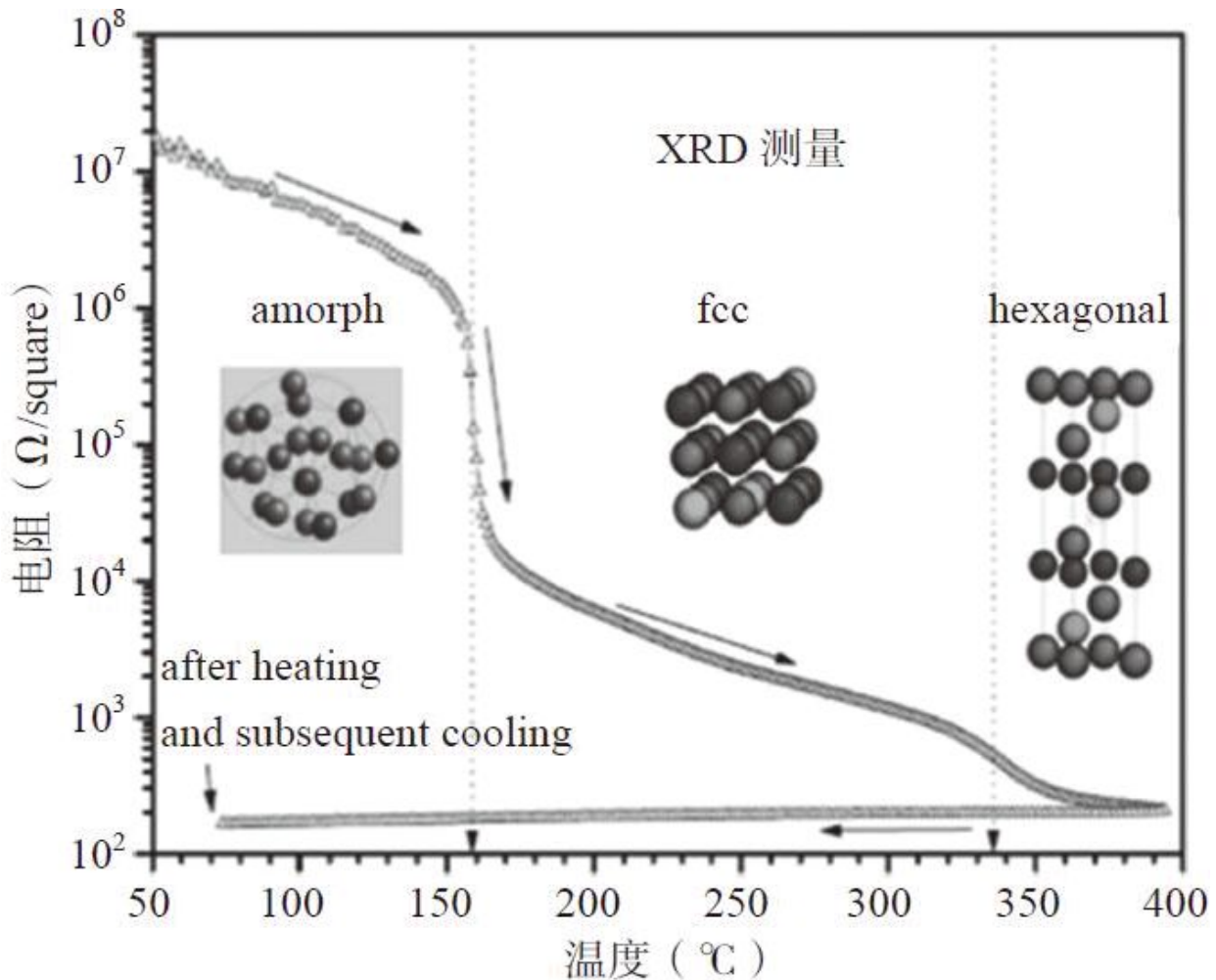


图3-26 GST材料状态随温度变化图

图3-27所示是一个PCM存储单元，读的时候我们只要测量GST上面金属节点的电压就知道了，晶体态时电阻低、电压低，无定形态时电阻高、电压高。其实测电阻就是测电压，假如底部接地，那么低阻时顶点电压低（和底部导通），可以表示“0”；高阻时隔断，顶点电压高，可以表示“1”。

那写怎么弄呢？图3-27所示中，柱子就是加热器，通过电流之后加热GST，导致它发生相变，不过在不同的温度下，经过一定时间，相变的结果不一样。如图3-28所示，高温 T_m 下短脉冲加热从晶体态变成

无定形态，较高温 T_x 长脉冲加热时从无定形态变成晶体态。图3-29所示是读写的温度时间控制波形。

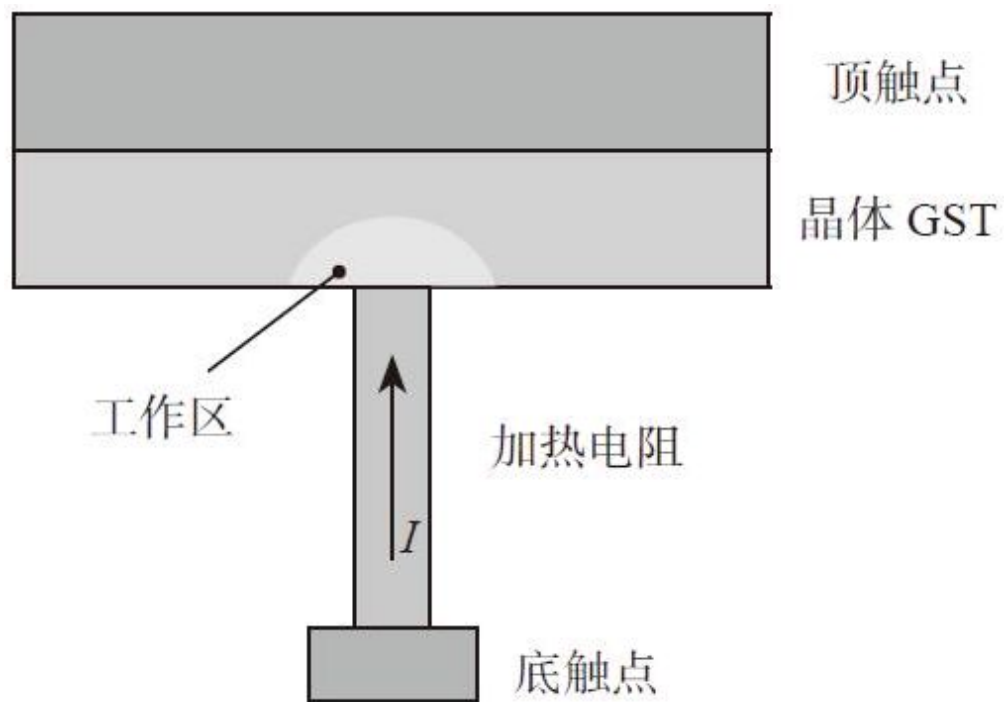


图3-27 PCM存储单元

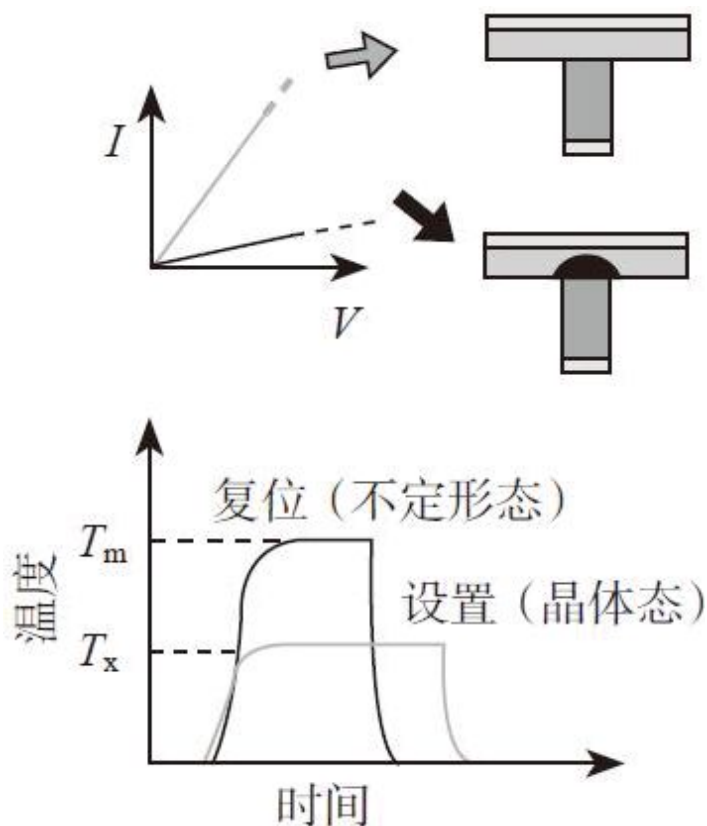


图3-28 不同温度脉冲对相变的影响

我们知道闪存里面有Bitline和WordLine，通过这两个组成的矩阵来管理上亿个存储单元。图3-30所示是PCM的Bitline和WordLine结构，通过两条线可以精确控制每一个单元。写的时候控制电流的大小来加热完成相变；读的时候通过测量Bitline的电压值就能知道是低阻还是高阻，从而获得0、1值。

要了解更多，请查看Numonyx公司Greg Atwood写的论文《Phase Change Memory: Development Progress and System Opportunities》和dailytech网站上Jason Mick写的博客《Exclusive: If Intel and Micron's "Xpoint" is 3D Phase Change Memory, Boy Did They Patent It》。

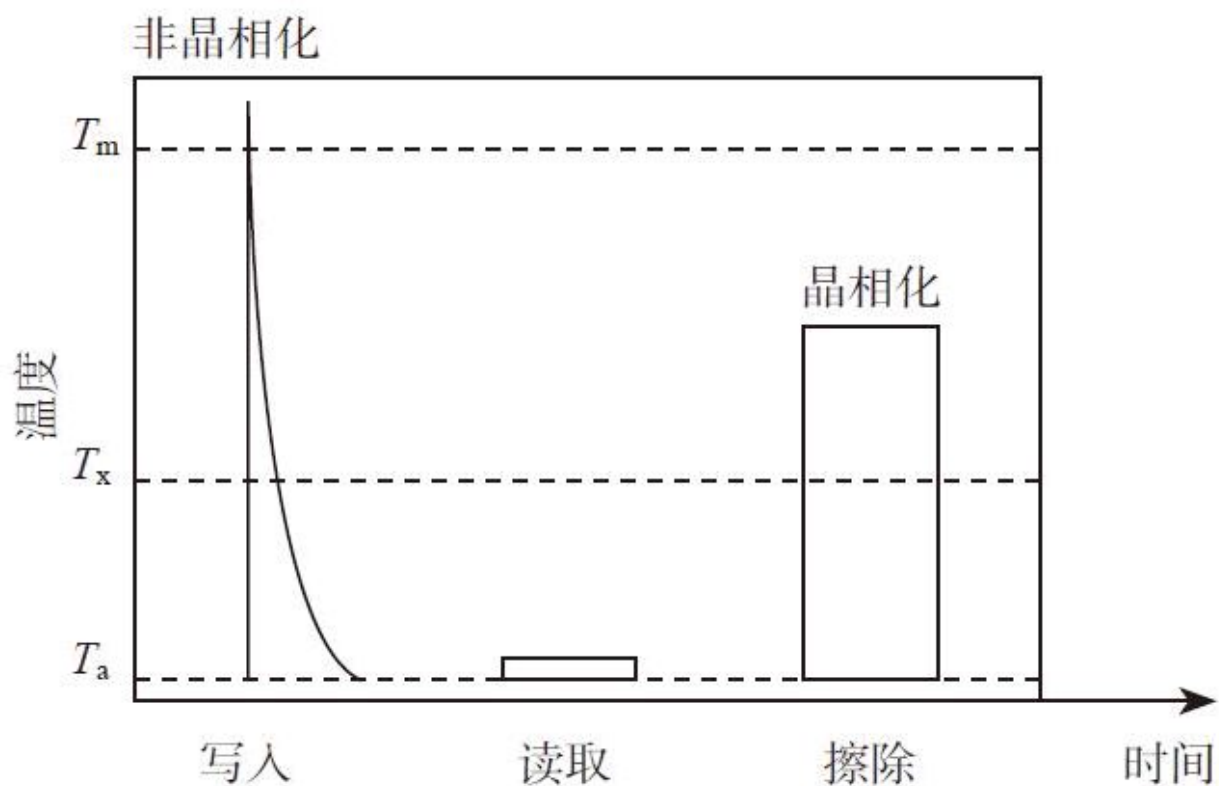


图3-29 读写操作通过温度时间控制完成功能

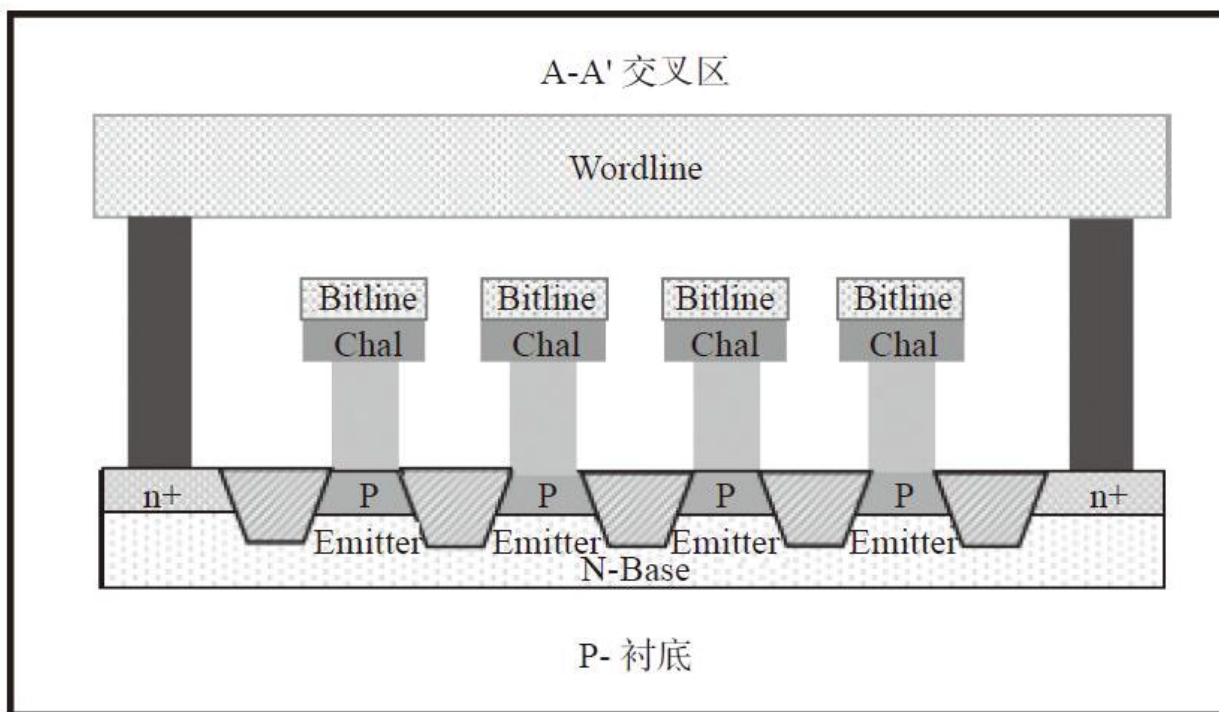


图3-30 PCM组织结构

3.2 闪存实战指南

3.2.1 异步时序

闪存接口有同步异步之分，一般来说，异步传输速率慢，同步传输速率快。异步接口没有时钟，每个数据读由一次RE_n信号触发，每个数据写由一次WE_n信号触发。同步接口有一个时钟信号，数据读写和时钟同步。

我们先来看看ONFI2.3协议规定的一个典型的闪存芯片管脚图（见图3-31）。这个芯片对外输出数据位宽为8bit，Ssync是同步，Async是异步。

比较一下两种接口下的管脚定义，大部分都是一样的，区别就是表3-4中所示的四类信号。后面我们看看同步和异步的时序就能了解为什么这些信号不一样了。

先来看看异步数据写入的时序图（见图3-32）。

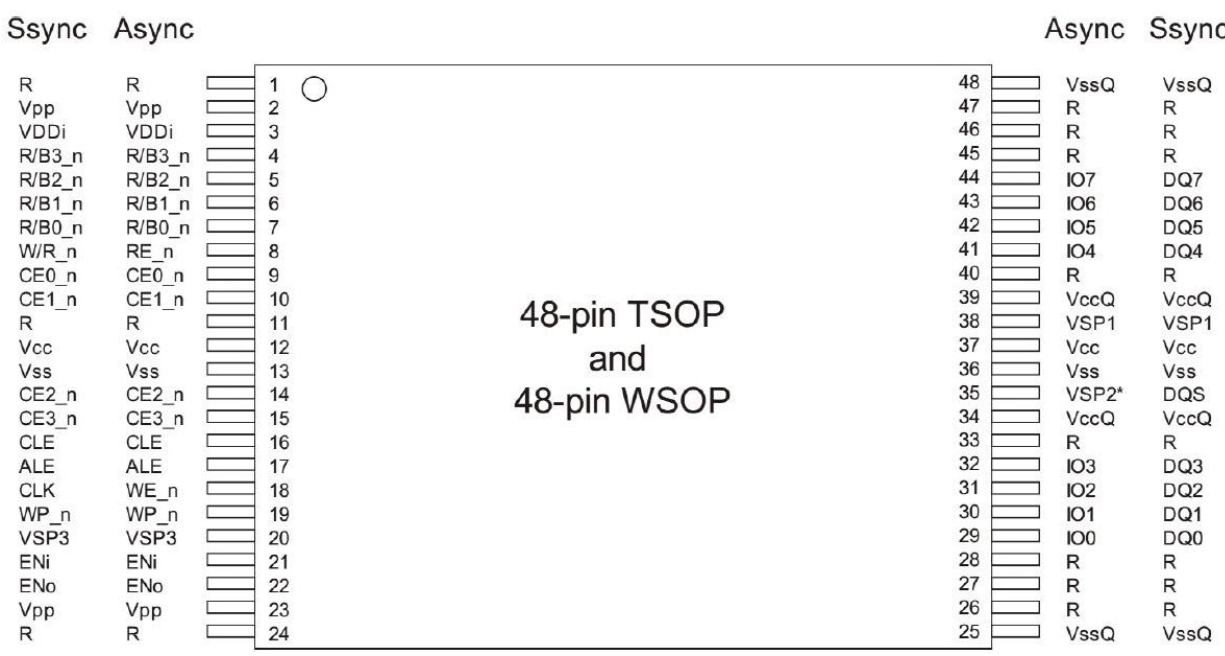


图3-31 闪存芯片管脚图
表3-4 同步异步管脚定义对比

同步	异步	同步	异步
W/R_n	RE_n	IO7-0	DQ7-0
CLK	WE_n	VSP2	DQS

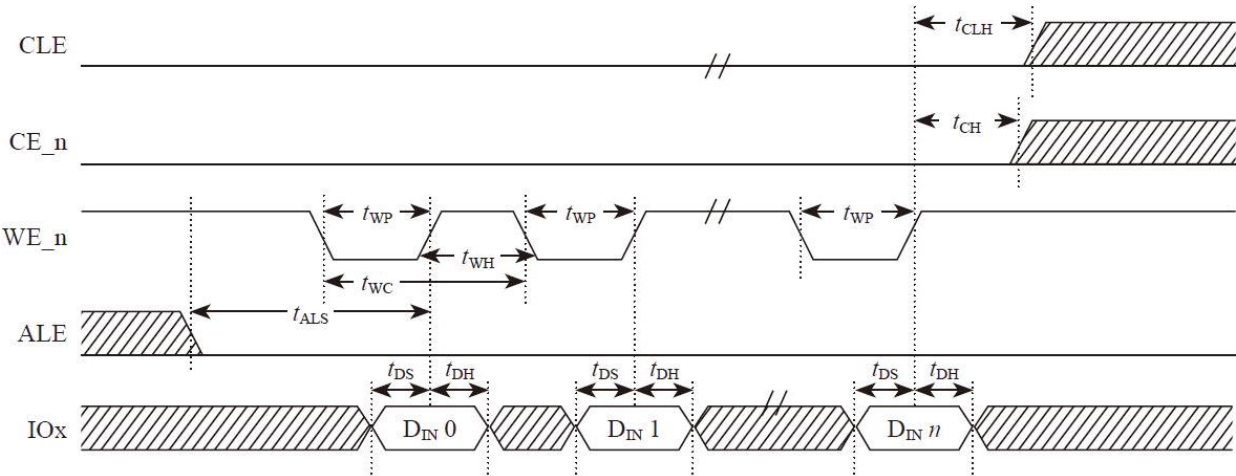


图3-32 异步写数据时序图

上图中有5个信号：

- CLE: Command Latch Enable，CLE有效时IOx发送命令。

- CE_n: Chip Enable，这个信号用来选通一个逻辑上的芯片——Target。为什么说是逻辑上的芯片？因为物理芯片里面封装了很多Target，每个Target都是完全独立的，只是有可能共享数据信号，所以通过CE_n来选择当前数据传输的是哪个Target，业内一般把Target叫作CE。

- WE_n: Write Enable，写使能，这个信号是用户发给闪存的，有效时意味着用户发过来的写数据可以采样了。

- ALE: Address Latch Enable，ALE有效时IOx发送地址。

- IOx: 数据总线。

同时有很多时间参数，这里只介绍几个关键的参数：

- t_{WP}：WE_n低电平脉冲的宽度。

- t_{WH}：WE_n高电平保持时间。

· t_{WC} ： t_{WP} 与 t_{WH} 合起来一个周期的时间。

· t_{DS} ：数据建立时间，意思就是8bit数据要都达到稳定状态，最多这么长时间。

· t_{DH} ：数据稳定时间，这段时间里数据信号稳定，可以来采样。

这样我们来看上面的时序图（见图3-32），数据写入的时候，数据总线不能传输地址和命令，所以ALE和CLE无效。这个Target有数据传输，所以CE_n有效。每一个WE_n周期对应一次有效的数据传输。

再来看看图3-33所示的异步数据读出时序，其中多了两个信号。

·RE_n：读使能。这个信号是用户发给闪存的，每发一个读使能，闪存就在数据总线上准备好数据，等用户采样；

·R/B_n：Ready/Busy。闪存正在进行内部读的时候，Busy_n有效，当操作完成且数据准备好之后，Ready有效，用户可以来读了。

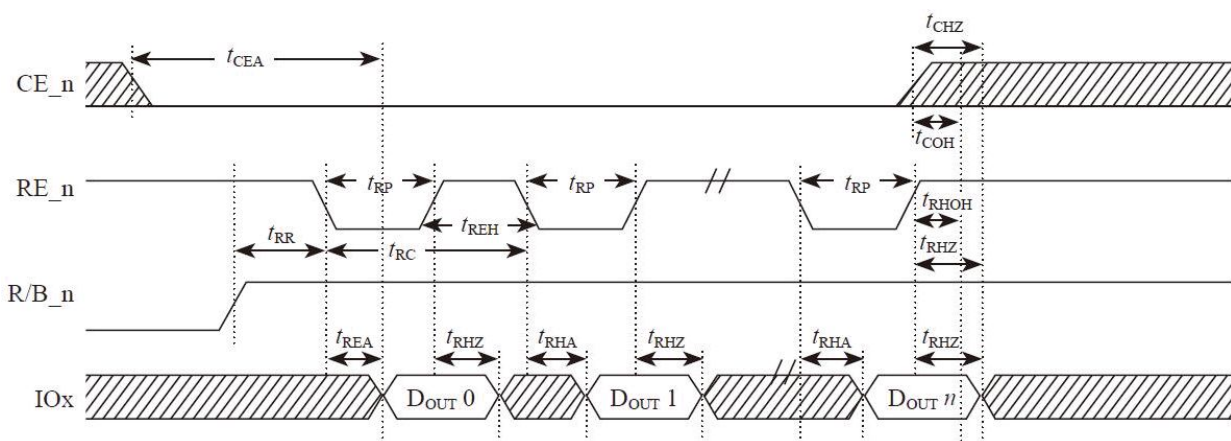


图3-33 异步读数据时序图

所以，用户向闪存发了读命令之后，Ready信号拉高，意味着数据准备好了。接着，用户发RE_n信号去读数据，每个RE_n周期，闪存发送一个有效数据到数据总线上，供用户采样，如图3-33所示。

3.2.2 同步时序

同步时序最重要的两个信号是时钟CLK和DQS。现在的闪存基本都采用了DDR（Double Data Rate）技术，就是说每个时钟周期传输两拨数据。图3-34是同步模式下的数据写入时序图，介绍一下几个信号。

- CLK：时钟。时钟信号由用户产生，在时钟信号的上升沿和下降沿都有数据被触发，实现DDR，意味着100MHz的时钟频率数据传输速率是200MT/s。

- W/R_n：Write/Read_n。写的时候高电平，读的时候低电平。

- DQS：Data Strobe。DQS用来区分出每个数据传输周期，便于接收方准确接收数据。读数据时，DQS由闪存产生，DQS上下沿和数据对齐。写数据时，DQS由用户产生，DQS中间对应数据的中间稳定区域。所以，DQS可以看成数据的同步信号。

- DQ[7: 0]：数据总线。

我们再来看看几个关键的时间参数。

- t_{CALS} ：CLE、W/R_n和ALE的建立时间。

- t_{DQSS} ：数据输入到第一个DQS跳变沿的时间。

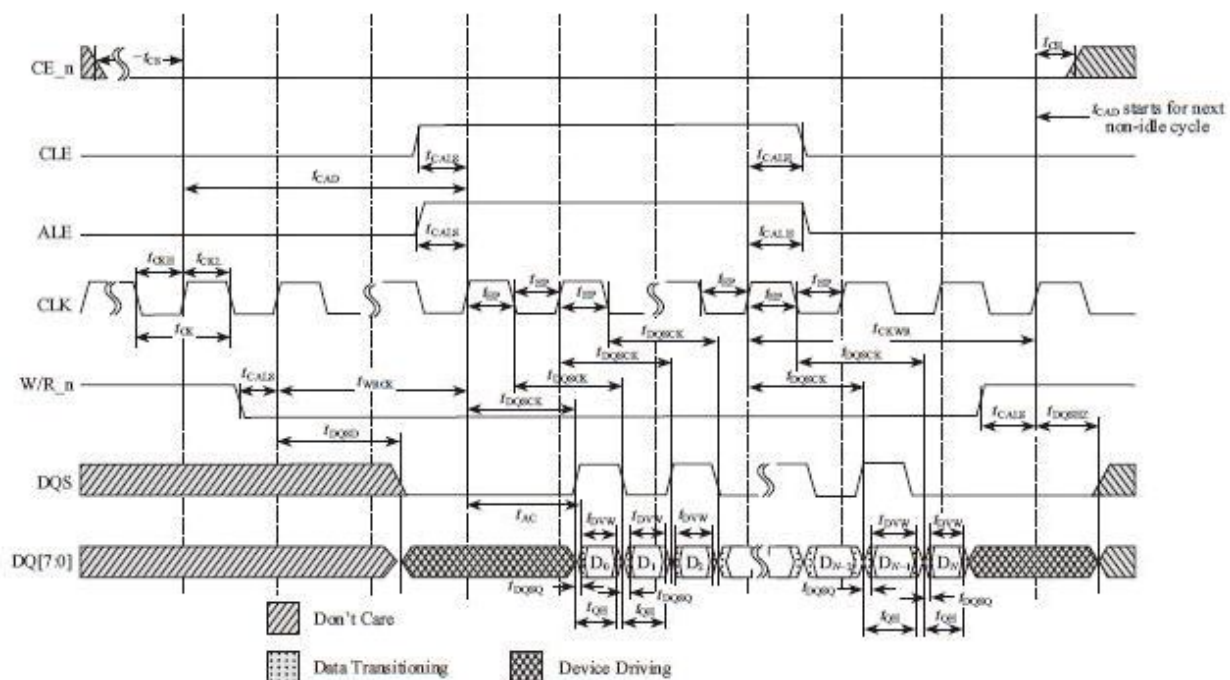


图3-35 同步读数据时序图

3.2.3 闪存命令集

固态硬盘主控是通过一系列闪存命令与闪存进行通信的。每款闪存芯片都定义了其支持的命令，以ONFI 2.3协议为例，它定义的命令如表3-5所示。用户要使用这些功能时发送命令即可，比如读数据，就发送00h~30h，不过具体命令时序和使用方式要看专门的定义。

下面介绍一下几个比较常用的命令：

- Read: 00~30h，读数据。读一个Page数据用这个命令。
- Read Multi-plane: 00~32h，同时读多个Plane的数据。多个Plane各读1个Page。
- Change Read Column: 05h~E0h，修改读列地址。Read命令从闪存介质读出一个Page的数据到闪存芯片里面的缓存，一个Page一般是8KB或者16KB，但是用户不一定需要所有数据，所以通过这个命令来修改传输数据的偏移地址。从某个Page内偏移地址开始进行数据传输。
- Block Erase: 60h~D0h，擦除一个Block。
- Read Status: 70h，查看最近一次操作的结果是成功还是失败。
- Read Status Enhanced: 78h，它和70h有什么区别？它是用在Multi-LUN操作的状态查看，可以指定查看哪个LUN的状态。
- Page Program: 80h~10h，写一个Page数据。
- Page Program Multi-plane: 80h~11h，同时写多个Plane的数据，写性能可以翻几倍。
- Read ID: 90h，可以读到在JEDEC注册的Manufacturer ID和Device ID。
- Read Parameter Page: ECh，可以读到这个CE的各种配置参数，比如支持ONFI的哪个版本，是否支持Multi-plane，异步或同步时序模式

是哪一种等。

•Get Features/Set Features: EEh/EFh，这两个命令给用户提供一个设定一些参数的接口，比如设置同步异步或者选择传输速率。

表3-5 闪存命令集

命令	O/M	第一周期	第二周期	命令	O/M	第一周期	第二周期
Read	M	00h	30h	Block Erase Multi-plane	O	60h	D1h
Read Multi-plane	O	00h	32h	Read Status	M	70h	
Copyback Read	O	00h	35h	Read Status Enhanced	O	78h	
Change Read Column	M	05h	E0h	Page Program	M	80h	10h
Change Read Column Enhanced	O	06h	E0h	Page Program Multi-plane	O	80h	11h
Read Cache Random	O	00h	31h	Page Cache Program	O	80h	15h
Read Cache Sequential	O	31h		Copyback Program	O	85h	10h
Read Cache End	O	3Fh		Multi-plane	O	85h	11h
Block Erase	M	60h	D0h	Small Data Move	O	85h	11h

(续)

命令	O/M	第一周期	第二周期	命令	O/M	第一周期	第二周期
Change Write Column	M	85h		Get Features	O	EEh	
Change Row Address	O	85h		Set Features	O	EFh	
Read ID	M	90h		Reset LUN	O	FAh	
Read Parameter Page	M	ECh		Synchronous Reset	O	FCh	
Read Unique ID	O	EDh		Reset	M	FFh	

不同的闪存所支持的命令有所差异。用户应该严格按照闪存芯片官方手册与闪存通信。

3.2.4 闪存寻址

了解基本命令的时序之前，我们再来复习一下闪存内部的结构。图3-36所示是一个Target，就是我之前说的一个可以独立工作的逻辑芯片。它包含2个LUN，每个LUN有2个Plane，每个Plane有很多Block，每个Block又有很多Page。

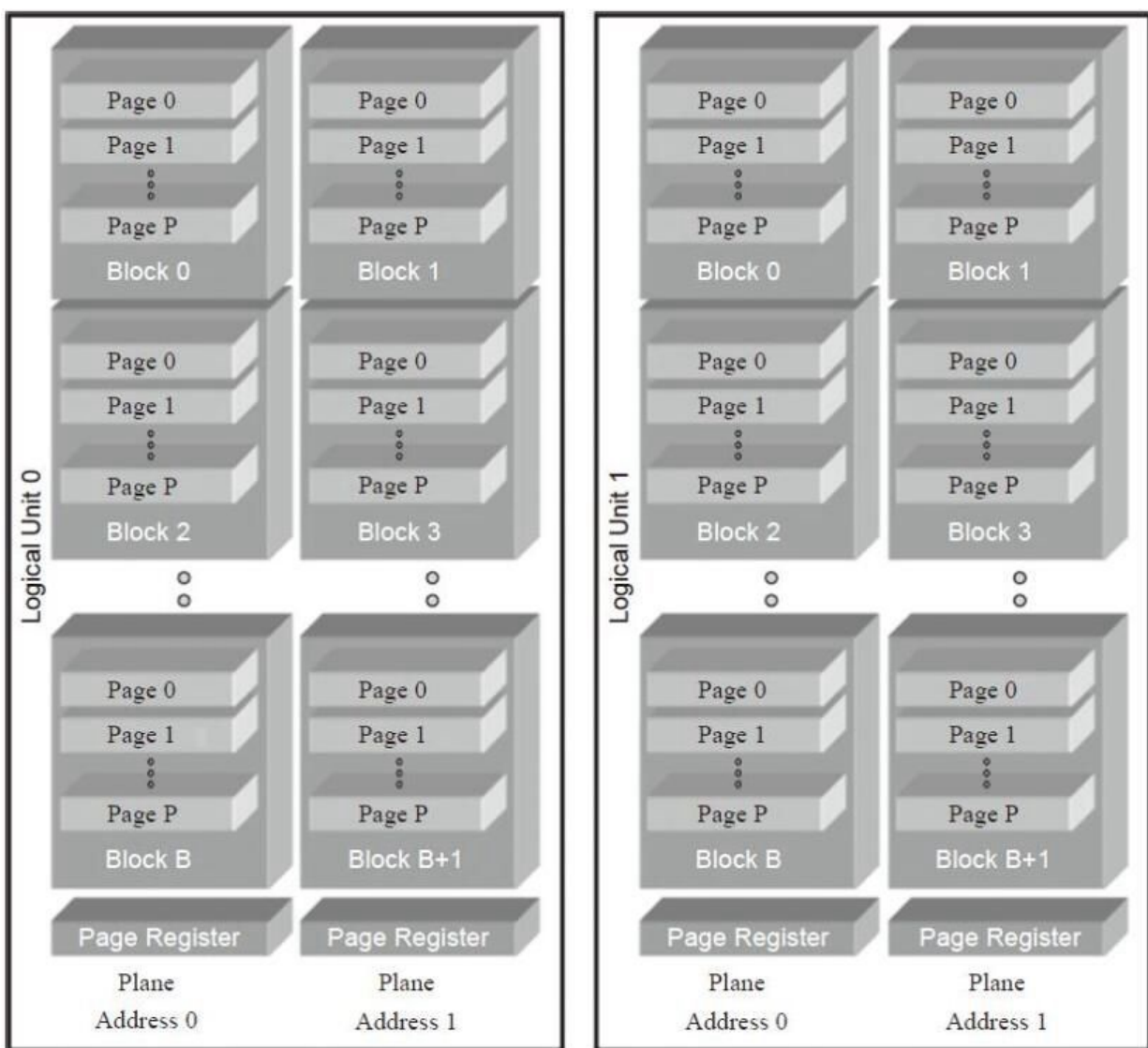


图3-36 闪存内部架构

为了访问这些资源，闪存里面使用了行地址（Row Address）和列地址（Column Address）。列地址就是Page内部的偏移地址。ONFI协

议中，行地址的定义如图3-37所示，从高位到低位依次为LUN、Block和Page地址，至于具体位宽，则和每个芯片的容量有关。

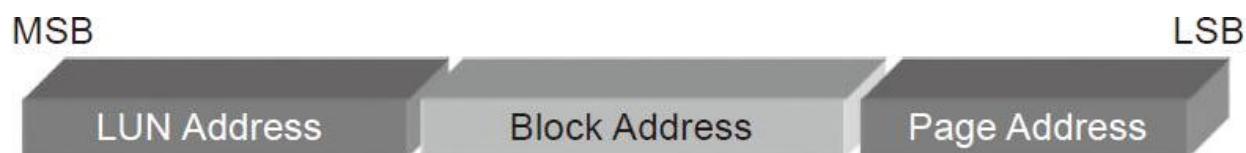


图3-37 闪存地址划分

估计你要开始问了：Plane在哪里？如图3-38所示，Plane是在Block地址的最低位。ONFI要求Multi-plane操作的时候，每个Plane的Page地址必须相同，Block地址不同的闪存要求不一样。比如Intel/Micron和东芝的闪存，在Multi-plane操作时，可以是不同的Block，但是三星的闪存，要求几个Plane操作的Block地址要相同。因为占的是Block地址的最低几位，所以进行Multi-Plane的时候，Plane一般有奇偶之分。

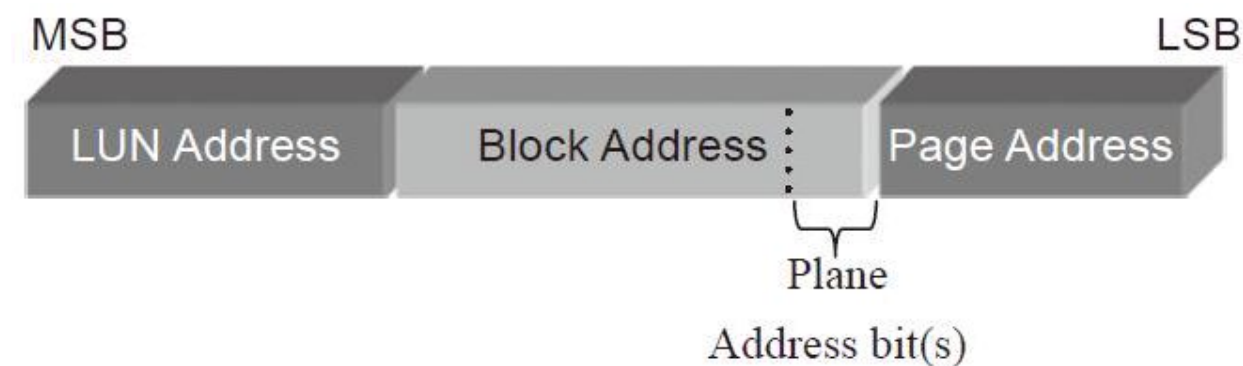


图3-38 Plane地址位

3.2.5 读、写、擦时序

读时序 如图3-39所示，在用户发送命令00~30h之间传输了所读的地址，包括2个列地址和3个行地址。发完命令后，SR[6]（Status Register，状态寄存器，bit 6）状态转为Busy，经过一段时间之后SR[6]状态转为Ready，数据就可以读了。

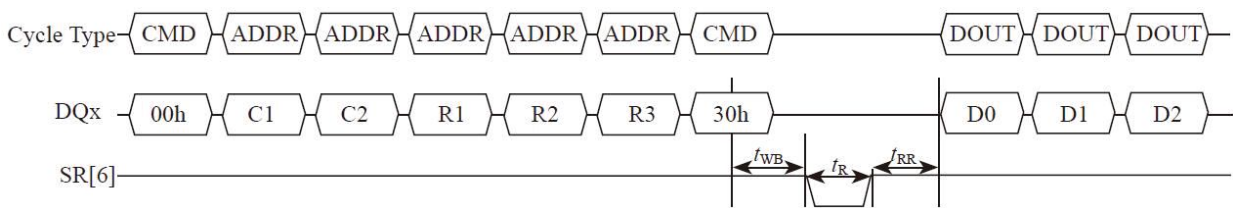


图3-39 读时序

写时序 如图3-40所示，用户发了80h命令之后，发送写地址，一般列地址是0，因为要把一个Page写满，如果不从头开始写满一个Page，往往会导致数据出错。发完地址tADL时间之后，开始传输数据到闪存的缓存。数据传完，发送命令10h，闪存芯片开始向介质写入数据，SR[6]状态为Busy，在写操作完成后状态转为Ready。

擦除比较简单，如图3-41所示，在命令60h和D0h之间发送LUN和Block行地址即可（因为擦除是以Block为单位）。

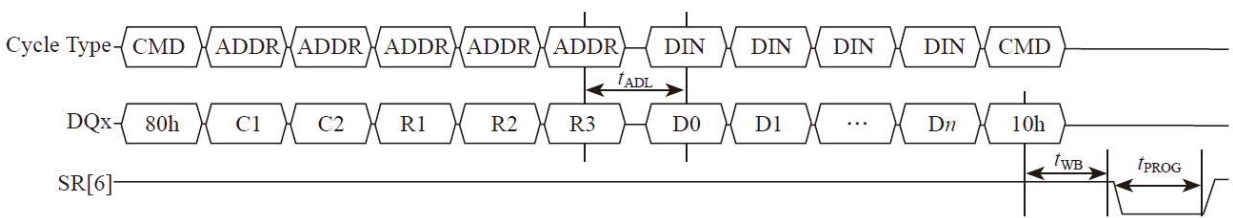


图3-40 写时序

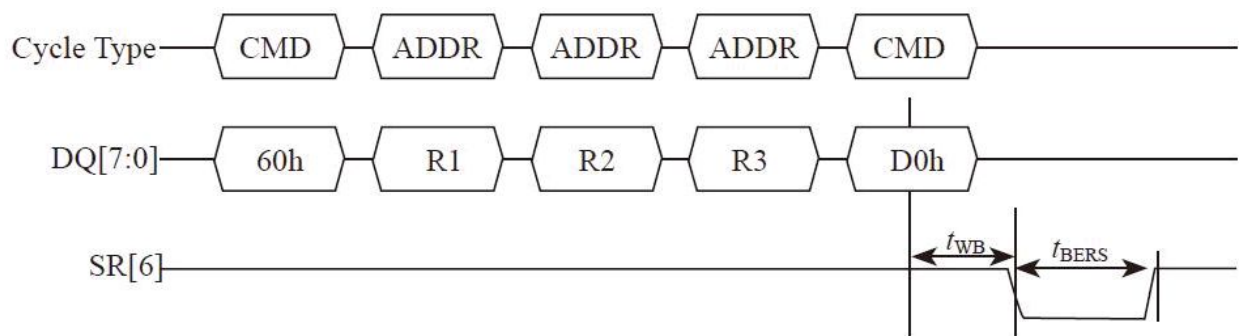


图3-41 擦除时序

3.2.6 ONFI与Toggle协议之争

前面讲的主要都是ONFI。事实上，闪存不只涉及ONFI协议，还有Toggle协议。

很久很久以前，闪存的相关技术长期垄断在三星和东芝两个大佬手里，其他的从业者日子过得不那么舒坦。

2002年，有个斯坦福的高才生苏秦，壮志满怀地去三星面试，结果因为气质不符没有被录取。他一气之下推掉了其他所有公司的邀请，回到河南老家每天闭门修炼。

三年以后，手机、MP3和U盘对闪存的需求量逐渐增大，消费类固态硬盘市场开始进入萌芽期，闪存的蛋糕越来越大，而当时各个闪存制造商的设计标准各有差异，这导致主控厂商和产品厂商各种麻烦，各种不适应。

苏秦觉得拯救苍生的时候到了，离开老家加入了Intel的战略发展部门，说服老板在当年旧金山的IDF上会盟天下诸侯，成立了ONFI（Open NAND Flash Interface）联盟，准备以合纵之法对付三星和东芝。

参加本次会盟的有：

- 闪存制造商：Intel、Micron、Hynix、Sandisk；
- 主控芯片厂商：LSI、Marvell、SMI、JMicron、Phison等；
- 存储产品厂商：Adata、Apacer、Biwin、Data I/O、HGST、Kingston、Netcom、Seagate、WD等；
- IP公司：Synopsys等。

三星和东芝坐拥函谷之利，占据了当时70%的市场份额。但是穿鞋的怕光脚的，面对ONFI咄咄逼人的气势，心里也是怕得要死。于是叫来双方共同的首席工程师张仪没日没夜地开会，最后拿出了连横作为对抗方案：

·三星允许东芝生产和制造自己旗下的OneNAND和Flex-OneNAND闪存芯片。

·东芝开放自己的LBA-NAND和mobileLBA-NAND闪存芯片技术给三星。

·同时计划一起研发新一代闪存产品，也就是后来的Toggle NAND。

其后的数年间，ONFI和Toggle两方你来我往，互为攻守。

2014年ONFI发布了4.0标准，最高速度达到了800MT/s。最新的Toggle标准最高速度也是800MT/s。

看上去ONFI比较牛，然而从市场份额上看，两大阵营几乎是五五开，三星/东芝还略占优势，如表3-6所示。

表3-6 闪存厂商市场份额对比

厂商	2015 年 4 季度营收 (百万美元)	市场份额	厂商	2015 年 4 季度营收 (百万美元)	市场份额
三星	2 792	33.6%	美光	1 154	13.9%
东芝	1 547	18.6%	SK 海力士	841	10.1%
西数 (闪迪)	1 311	15.8%	英特尔	662	8.0%

打打杀杀不容易，上个图，对比一下管脚定义，其实区别也没那么大（见图3-42）。

同步，异步模式共享管脚

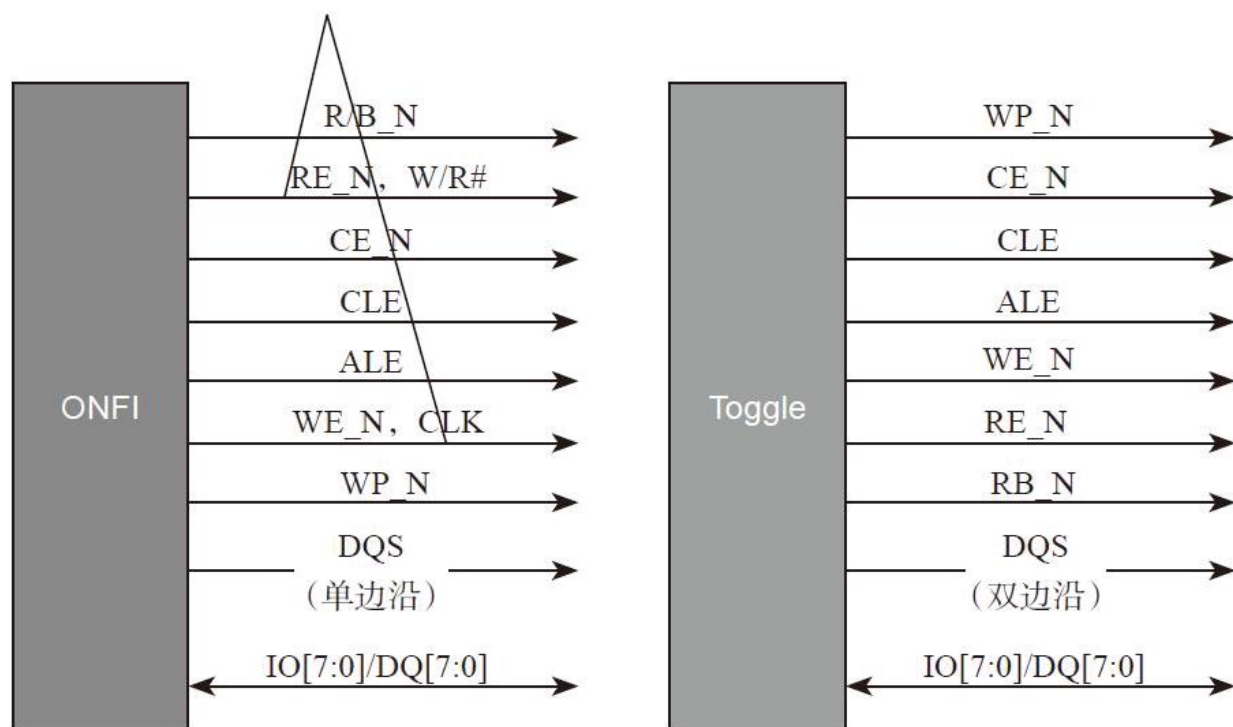


图3-42 ONFI和Toggle管脚定义对比

Toggle同步模式下不用时钟，写数据用DQS差分信号跳变沿触发，读数据根据主控发的REN差分信号跳变沿发送读请求，DQS跳变沿输出数据。

ONFI同步模式下有时钟，数据、命令、地址都要与时钟同步。但是DQS、Clock都不是差分信号，所以边沿容易受干扰。

ONFI 3.0里面有NV DDR2模式，这就和Toggle一样了，不再用Clock，用DQS和REN差分信号。

那么问题来了，他们会在周天子（JEDEC）的努力下最终走到一起吗？

3.3 闪存特性

3.3.1 闪存存在的问题

谈谈闪存的一些特点，或者说它作为存储介质面临的挑战。

1. 闪存坏块

闪存块（**Block**）具有一定的寿命，不是长生不老的。前面提到，当一个闪存块接近或者超出其最大擦写次数时，可能导致存储单元永久性损伤（见图3-43），不能再使用。随着闪存工艺不断向前发展，晶体管的尺寸越来越小，擦写次数也变得越来越少。

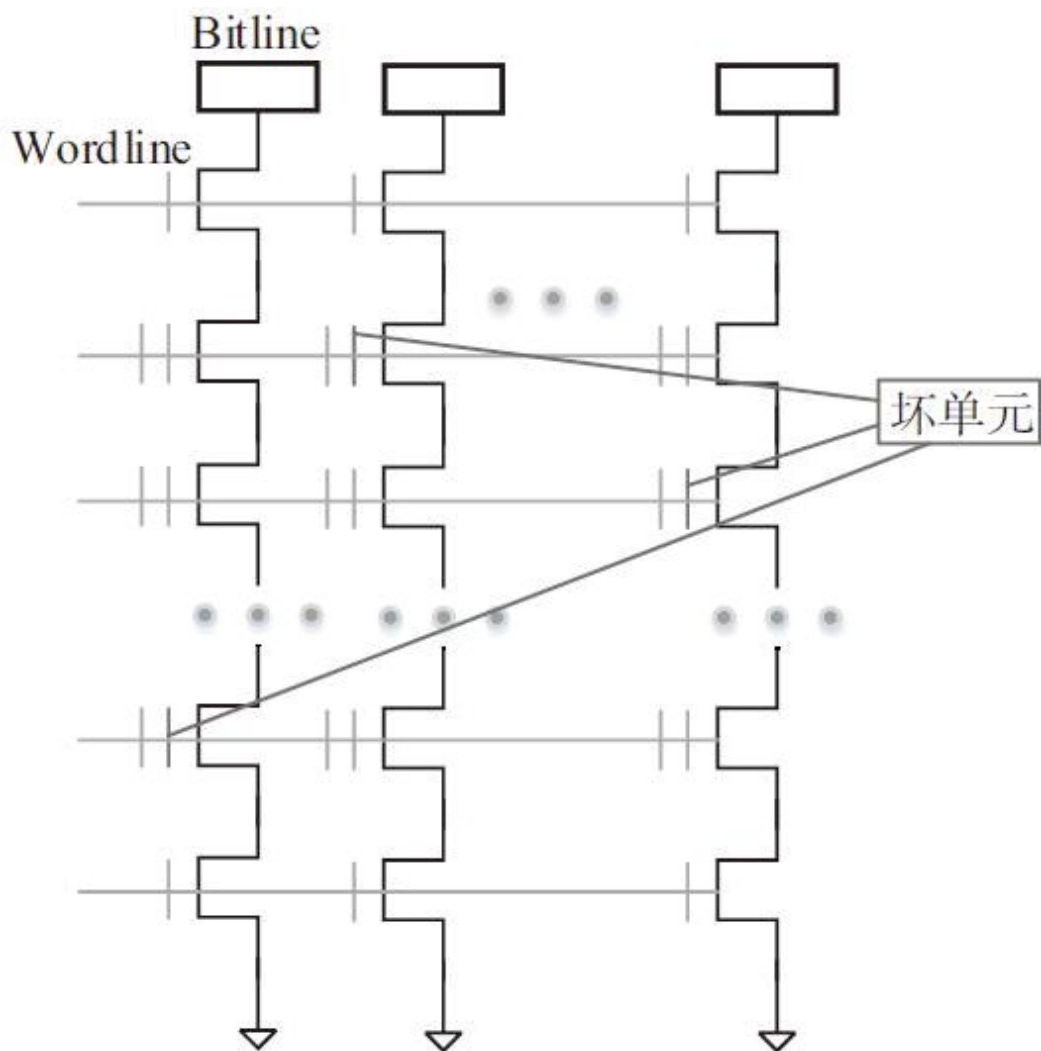


图3-43 闪存损坏状态

闪存中的存储单元先天就有一些是坏的，或者说的不稳定的。并且随着闪存的不断使用，坏的存储单元越来越多。所以，用户写入闪存的数据，必须要有ECC纠错码保护，这样即使其中的一些比特发生反转，读取的时候也能通过ECC纠正过来。但若出错的比特数超过纠错能力范围，数据就会丢失，对这样的闪存块，我们应该弃之不再使用。

闪存先天有坏块，也就是说有出厂坏块。并且，用户在使用过程中会新添坏块，所以必须有坏块管理机制。

2.读干扰

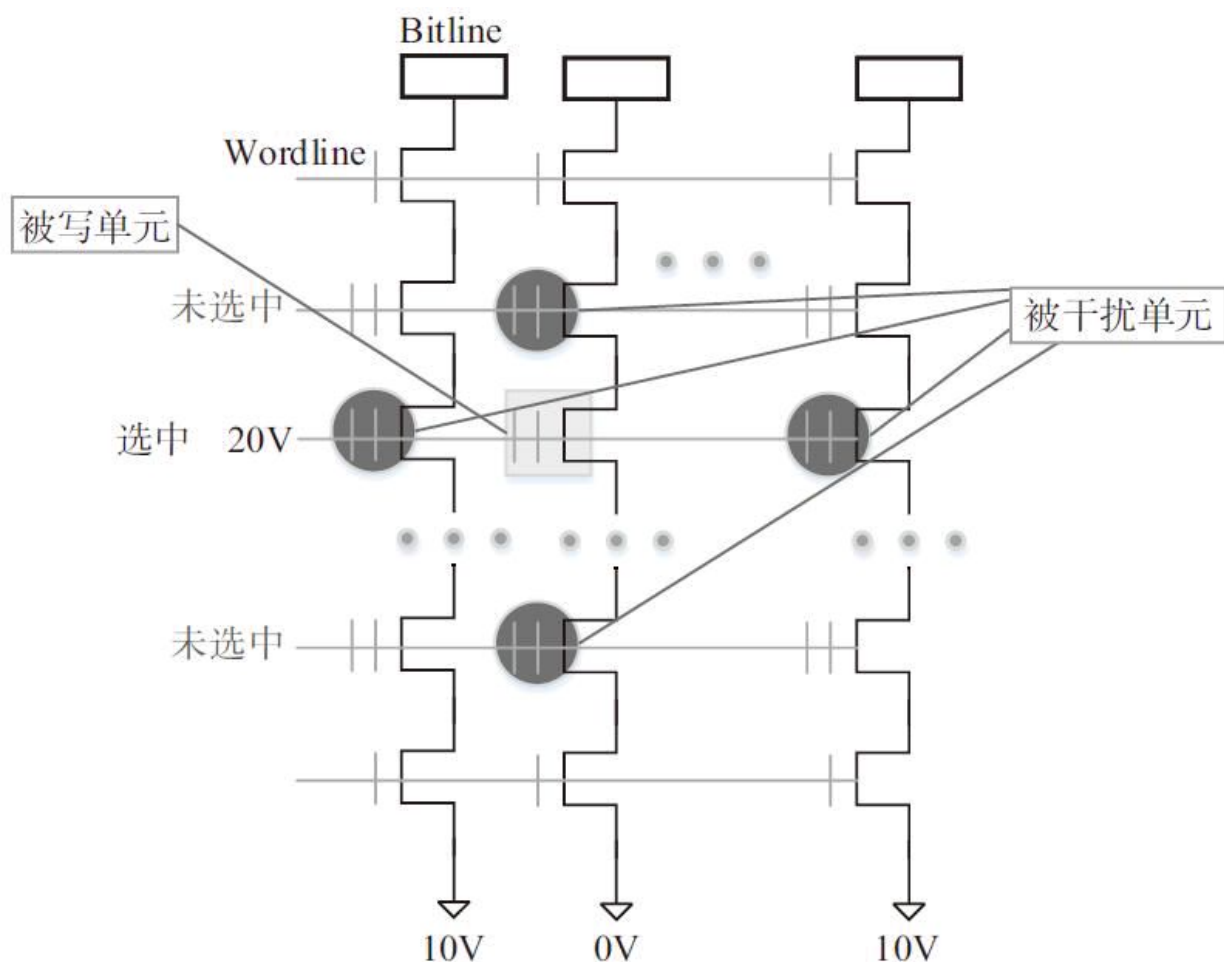


图3-45 写干扰原理

我们写一个闪存页的时候，数据是0和1混合的。由于擦除过的闪存块所有的存储单元初始值是1，只有写0的时候才真正需要操作。如图3-45所示，方框里的单元是写0，即需要写的，圆圈里的单元的代表写1，并不需要写操作。我们这里把方框里的单元称为**Programmed Cells**，圆圈里的单元称为**Stressed Cells**。写某个闪存页的时候，我们是在其Wordline控制极加一个正电压（图3-47中是20V）。**Programmed Cells**所在的String是接地的；不需要写的单元所在的String接一个正电压（图3-47中为10V）。这样最终产生的后果是，**Stressed Cell**也会被轻微写。与读干扰不同的是，写干扰影响的不仅是同一个闪存块当中的其他闪存页，自身闪存页也会受到影响。相同的是，都会因不期望的轻微写导致比特翻转，都会产生非永久性损伤，经擦除后，闪存块还能再次使用。

4.存储单元间的耦合

还有一个问题，就是存储单元之间的耦合影响（Cell-to-Cell interference）。前面提到，浮栅极闪存存储电荷的是导体，因此存储单元之间存在耦合电容，这会使存储单元内的电荷发生意外变化，最终导致数据读取错误。

5.电荷泄漏

存储在闪存存储单元的电荷，如果长期不使用，会发生电荷泄漏。这同样会导致非永久性损伤，擦除后闪存块还能使用。

上面说的这些，是所有闪存面临的问题，包括SLC、MLC和TLC，这些问题的处理方法在第4章会进行介绍。不同商家的闪存、不同制程的闪存，以及2D/3D闪存，还有其特有的问题，用户在使用时需要用固件克服或者缓解这些问题。

3.3.2 寿命

我们再来看图3-46这张0和1的分布图，横轴是电压，纵轴是存储单元的数量。0的区域表示被写过的那些单元电压分布区间，1的区域是被擦过的那些单元电压分布区间。所以说，如果要正确地读到数据，0和1这两个区间要尽量分割清楚，保证它们的主峰之间有足够远的距离。除此之外，阈值电压也不能太偏。回忆一下读数据的原理。

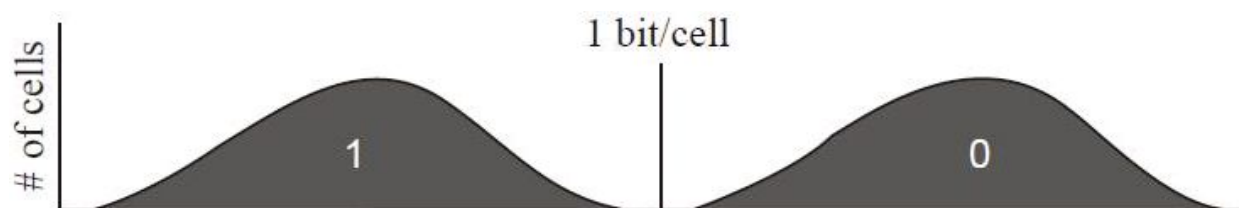


图3-46 SLC电压分布

要读的单元栅极加0V电压，这时擦过的晶体管阈值电压是 $-V_t$ ，导通，沟道有电流，Bitline端的传感器能够检测到，读到“1”。而经过写的晶体管阈值电压是 $+V_t$ ，不导通，沟道电流很小，读为“0”。随着擦写次数的增加，会发生3种故障：

- 擦过的晶体管阈值电压变大，从 $-V_t$ 向0V靠近，这样读的时候沟道电流变小，传感器检测不到，读出错。

- 写过的晶体管阈值电压变小，从 $+V_t$ 向0V靠近，有可能会被误检测为擦过的状态。

- 写过的晶体管阈值电压变大（如图3-47所示， $>5V$ ，即使控制极加5V电压，它也是截止的），有可能在其他的单元读的时候，把整个Bitline都给关了。

产生不少Charge Trap，这些陷阱会吃掉电子，导致写之后，进入浮栅的电子数量会减少，最终的结局就是0和1两个区间不断靠近。

如图3-48所示，上面是写后的阈值电压，下面是擦除后的阈值电压，很明显，擦除后的阈值电压在擦很多次之后显著变高。所以，一般擦除之后会做校验，方法是把所有的Wordline设为0V，再去检测每个Bitline的电流。如果某个Bitline电流是0，就意味着有个单元的擦除阈值电压接近0V，导致晶体管关断。所以这个闪存块应该标为坏块。

了解了闪存寿命的原理之后，我们再来看看固态硬盘设计实践中怎么解决这个问题。一般有以下方法：

- Wear Leveling：通过磨损平衡算法，让所有的闪存块均衡擦写，避免少数闪存块先挂掉，导致固态硬盘容量下降。

- 降低写放大：写放大越低，固态硬盘的磨损速度越慢。

- 用更好的纠错算法：纠错能力越强，容许的出错率越高，故采用更好的纠错算法可以延长硬盘使用寿命。

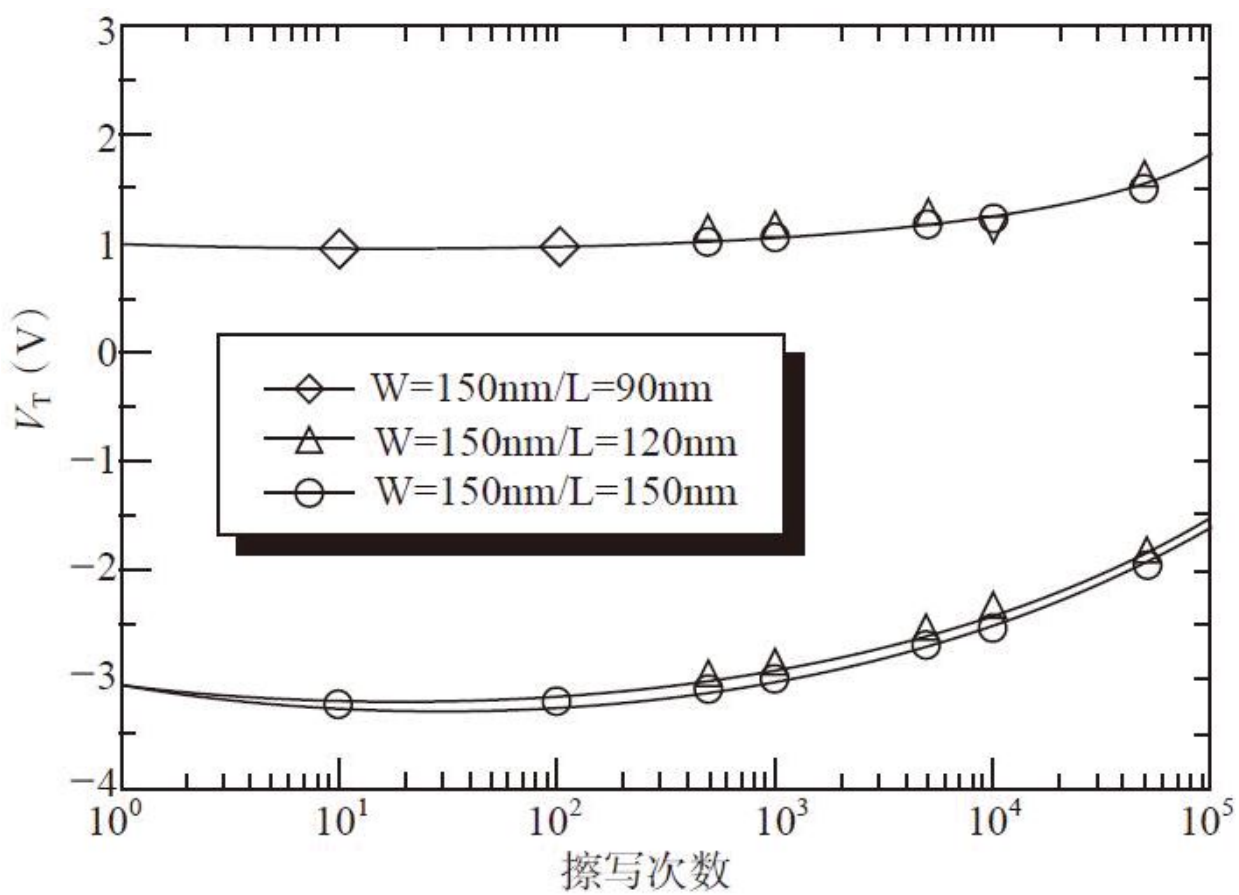


图3-48 阈值电压变化图

3.3.3 闪存测试

为什么固态硬盘还涉及闪存测试呢？这不应该是闪存厂商的事情吗？如果你问这些问题，那就是很傻很天真。理论和现实总是有差距的，固态硬盘内部需要对闪存做测试，原因是：

- 闪存厂商卖给你的闪存不一定是好的，总是有概率存在故障芯片；

- 固态硬盘制造过程中有合格率问题，不能保证每个闪存芯片都焊接得完美无缺；

- 固态硬盘制造商为了降低成本，会从各种渠道获得低价闪存芯片，这些芯片质量没有保障，需要固态硬盘制造商自己筛选。

图3-49所示是BGA封装的焊球X光片，可以看出里面有个空洞，导致电路信号故障。所以，固态硬盘出厂前要对每一块闪存进行测试，测试方法如下：

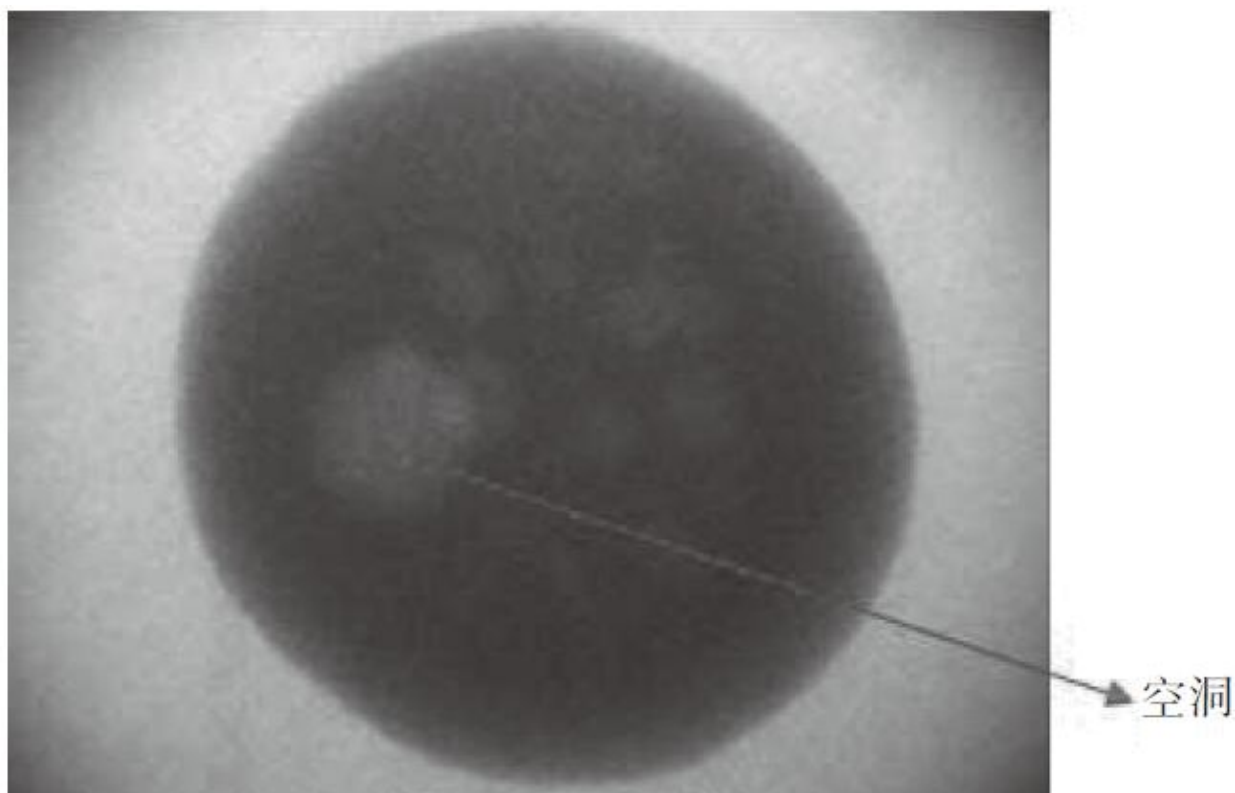


图3-49 BGA焊接空洞

- 测试每个CE是否可以正常操作，比如Reset、Read ID等；

- 对每个LUN、Plane进行读写测试，要考虑到一定的比特翻转率，看看写入的数据和读出差距有多大。写入数据要选择不同的数据类型，比如连续的0或者连续的1。存储器件测试有很多专用数据格式，有兴趣的读者可翻看各种论文，也可以参考著名的内存测试软件memtest的测试方法。

如果工厂发现闪存有问题，那该怎么办？还能怎么办，换好的呗。把芯片拆下来，再换个好的上去，对熟手来说轻轻松松。如果是BGA封装，需要专业设备辅助。那么换下来的芯片就这么扔了吗？能变废为宝吗？肯定能，比如放到U盘里。

一般来讲，从U盘到消费级固态硬盘再到企业级固态硬盘，对闪存的要求是逐渐升高的，因为写的强度不断增大。U盘也就偶尔用用，一天写不了多少数据。自己笔记本平时也不会一直写数据。企业级固态硬盘几乎每时每刻都在工作，读读写写，忙个不停。所以，不要以为几个U盘就能凑一个固态硬盘使用，闪存的质量是不一样的。企业级固态硬盘用的是最贵的原厂闪存，消费级固态硬盘往往是便宜的，有很多厂家从闪存厂商购买晶圆自己封测。U盘就是最差的闪存了，其所用芯片来自于各种渠道，成本很低。

3.3.4 MLC使用特性

对MLC来说，擦除一个闪存块的时间大概是几毫秒。闪存的读写则是以闪存页为基本单元的。一个闪存页大小主要有4KB、8KB、16KB几种。对MLC或者TLC来说，写一个闪存块当中的闪存页，应该顺序写Page0、Page1、Page2、Page3.....禁止随机写入，比如Page2、Page3、Page5、Page0.....为什么？原因主要有二：

- 一个存储单元包含两个闪存页数据，要先写Lower Page，再写Upper Page。

- 相邻单元之间有耦合电容，工艺上要求后面的闪存页写操作时前面的闪存页已经写过。

但对读来说，没有这个限制。SLC也没有这个限制。

MLC有其特有的一些问题：

- 正如前面提到的，MLC最大擦写次数会变小。这样，就更需要Wear Leveling技术来保证整个存储介质的使用寿命。

- 对MLC来说，一个存储单元存储了2bit的数据，对应着两个Page：Lower Page和Upper Page。假设Lower Page先写，然后在写Upper Page的过程中，由于改变了整个单元的状态，如果这个时候掉电，那么之前写入的Lower Page数据也会丢失。也就是说，写一个闪存页失败，可能会导致另外一个闪存页的数据损坏。

- 前面说到，不能随机写。不能先写Upper Page，然后再写Lower Page，这点就限制了我们不能随意地写。

- 写Lower Page时间短，写Upper Page时间长，所以会看到有些闪存页写入速度快，有些闪存页写入速度慢。

关于MLC的Lower Page数据损坏问题，阿呆还想多说一些，这个问题其实对于固态硬盘控制器的设计者来说是个大问题，因为涉及数据可靠性。首先我们来说两条存储行业的规矩：

·一般在没有盘内缓存的情况下，我们认为写到硬盘的数据如果已经返回写成功，那么这个数据就是安全的。数据写到物理介质上就可以放心了。

·如果数据在写的过程中发生了异常掉电，那么该数据即使丢了也可以接受，毕竟用户认为数据还没写完。

但是**Lower Page**数据损坏打破了这个常识：尽管已经成功写到了盘里，但是假如该数据位于**Lower Page**上，很不幸的是，恰好过了不久，后面有数据写对应的**Upper Page**时发生了异常掉电，那就会导致**Lower Page**上已经写好的数据也被破坏。也就是说，固态硬盘正在写的时候，如果发生了异常掉电，有可能会丢失之前写入的数据。

那该怎么办呢？聪明的消费级固态硬盘研发工程师采用了很多技术来防止这种情况发生。

·只写**Lower Page**：成本比较高，只适合关键数据和土豪。

·**Lower Page**和**Upper Page**打包写：每次数据量多凑点，争取**Lower Page**和**Upper Page**都写（需要闪存支持**One Pass Programming**）。

·定期填充**Upper Page**：消费级固态硬盘要求省电，所以会频繁进入省电模式，可能安静个几百毫秒就自动休眠了。休眠之前检查是不是有**Lower Page**写过了，有**Upper Page**还没写的情况，就把**Upper Page**也写一下。

·写**Lower Page**数据时，备份该数据到别的闪存块上，直到它对应的**Upper Page**数据写完。这样即使掉电导致**Lower Page**数据丢失，也可使用备份数据进行还原。

·**MLC**闪存块当**SLC**块使用，强迫用户数据写到**SLC**块，随后以垃圾回收的方式把数据从**SLC**闪存块搬到**MLC**闪存块。

经过上述各种努力，用户的数据可以做到很安全，**Lower Page**数据损坏的危害会降到最低。所以，请你放心，使用固态硬盘是安全的！

对企业级固态硬盘来讲，数据安全性尤其重要，而且要长期开机，不能像消费级一样动不动就进入省电模式。那么，怎样降低**Lower Page**数据损坏的危害？一般是在固态硬盘内配备大电容，发生异常掉电后，大电容储存的电量可以支撑几十毫秒，保证正在进行写操作的闪存把数据写完。现在主流的企业级固态硬盘控制器不仅能在大电容供电的时间内把闪存正在写的数据写完，还能把缓存里的数据写完，最后写一些固态硬盘内部的关键管理数据，比如映射表等。

3.3.5 读干扰

记得几年前我们碰到一个问题，就是有客户反映，他们在使用我们的固态硬盘时，发现读性能过段时间就有一个比较大的下降。后来，经过我们工程师的努力，发现罪魁祸首就是读干扰（Read Disturb）。最后，聪明的工程师完美地解决了这个问题。

读干扰为什么会导致性能下降？下面将解释原因。

读干扰会导致浮栅极进入电子。由于有额外的电子进入，会导致晶体管阈值电压右移（Data Retention问题导致阈值电压左移），如图3-50所示。

由于晶体管阈值电压偷偷发生了变化（变大了），闪存内部逻辑如果还是按照之前的参考电压加在控制极上然后去判断数据，肯定会发生误判，也就是读到错误的数据。

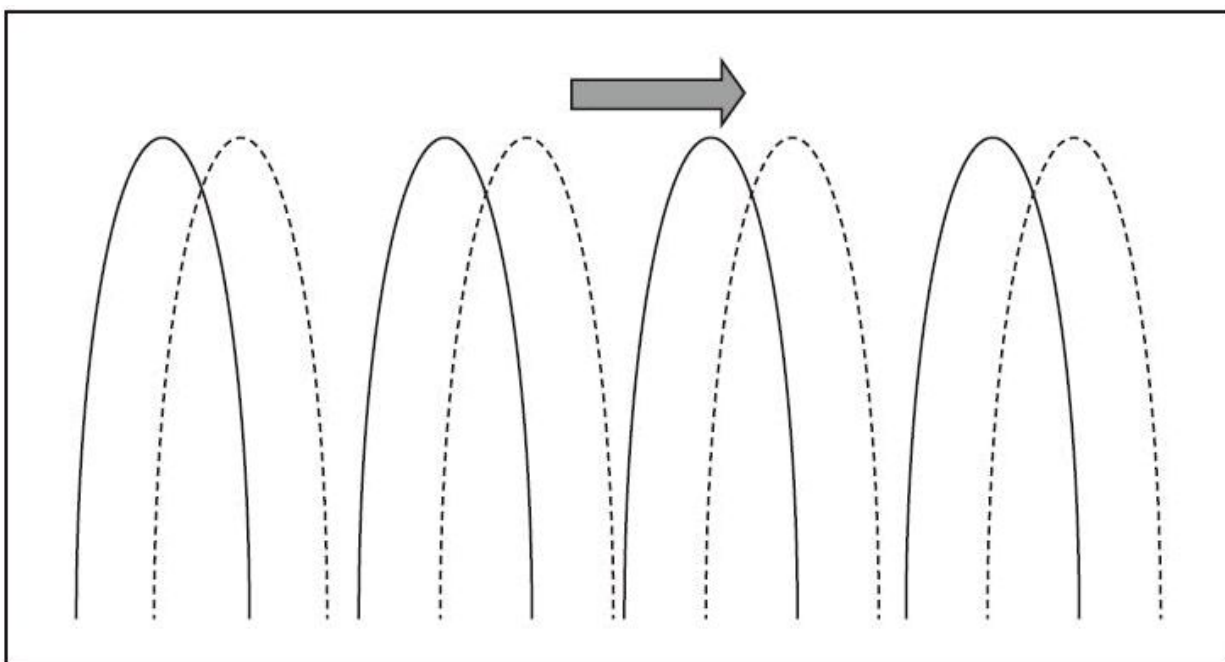


图3-50 阈值电压偏移

阈值电压右移的速度，也就是读干扰影响数据的程度，一方面与读该闪存块上数据的次数有关，读得越多，右移越多，影响越大；一

方面还跟闪存块的擦除次数有关，擦写次数越多，绝缘效果越差，电子进入浮栅极就越容易，读干扰的影响也就越大。

那么，闪存使用者如何应对读干扰呢？

一般做法是记录每个闪存块读的次数，赶在这个数值达到阈值（闪存厂家提供）之前，把闪存块上所有的数据刷新一遍（读出来，擦除，然后写回），或者把数据搬到别的地方。回到开头那个问题，读干扰为什么会致固态硬盘性能下降？就是因为一个闪存块上的数据读的次数太多了，固件需要赶在数据出错前，把整个闪存块数据刷新或者搬移，避免数据出错，但这会占用底层带宽，导致主控读写性能下降。

还有人研究发现，减小 V_{pass} （加在没有被读的那个Wordline上的电压）可以缓解读干扰。因为 V_{pass} 变小，电场减弱，吸入电子的能力减弱，自然能缓解读干扰的影响。但是，一方面，现在闪存厂商都没有开放调 V_{pass} 电压的接口给用户；另一方面，过低的 V_{pass} 可能导致读失败。该方法只能起到缓解作用，不能从源头上杜绝读干扰的影响。

3.3.6 闪存数据保存期

下面来聊聊存储的数据能保存多久。

图3-51是现藏于甘肃省博物馆的西汉天水放马滩地图，于1986年在甘肃天水放马滩5号汉墓出土，其用纸是世界上现存最早的纸。根据考古专家的断定，这是一张西汉文帝或景帝（公元前179年—前143年）时期的纸质地图。距今已经有两千多年的历史，变得残破不全。

刘慈欣的小说《三体》中提到，即使是刻在岩石上的巨型文字，经过几千万年的沧海桑田，也会找不到踪迹。

所以，无论用任何存储技术，存储的数据都不能永远保存，都会有个保存时间。闪存中，数据保存时间的问题叫作**Data Retention**。到了期限，数据就会出错，标志就是从闪存读出来的数据无法用**ECC**纠错成功。我们知道闪存一般有以下错误：

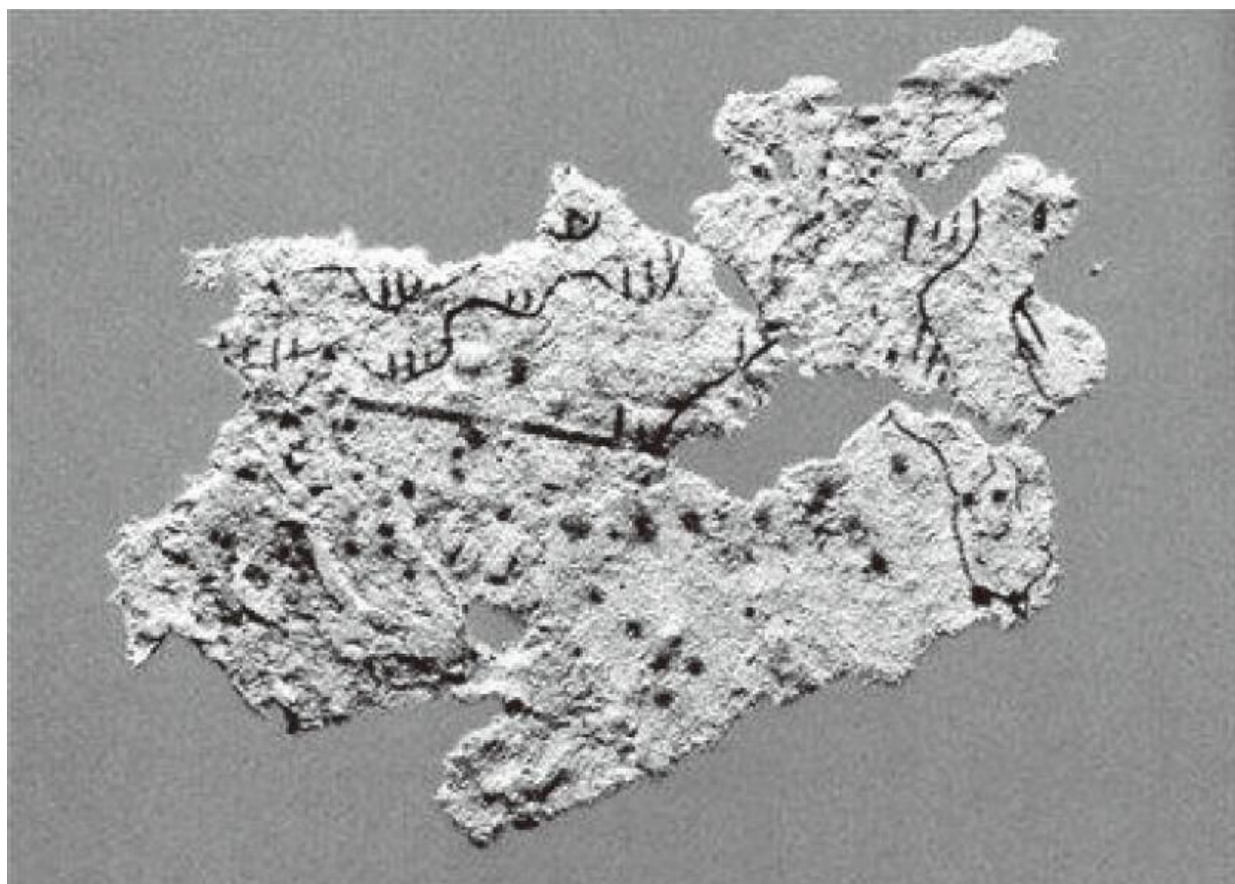


图3-51 世界上最早的纸

·电气问题：比如虚焊或者芯片故障，导致正常命令无法执行或者数据错误率异常高。这种问题在闪存或固态硬盘出厂测试时就会被发现。

·读、写、擦失败：基本命令执行失败，通过状态位可以读到结果。这些问题在芯片使用过程中也有可能发生，但是概率非常小。

·ECC纠错失败：其实就是数据错误率太高，超过了纠错算法的纠错能力。**Data Retention**是其中一个元凶。

闪存存储的机理是通过量子隧道效应，电子跃迁到浮栅层并停留在那里。随着时间的流逝，电子还是有一定概率离开浮栅层，回到沟道里面，离开的电子多了就有可能导致写过的单元读出来的结果跟擦除过的一样，也就是说数据出错了。**Data Retention**和浮栅层下面的氧化层厚度有关，毕竟氧化层越厚，电子离开的概率越小。有研究表明，氧化层厚度如果是4.5nm，那么理论上数据可以保存10年。

SSDFans微信群里有一位大牛群友蔡宇（Yu Cai）博士，他在Carnegie Mellon University攻读博士时专门研究闪存纠错，后来去LSI做这方面的研发。阿呆这次根据他的一篇论文《Data Retention in MLC NAND Flash Memory: Characterization, Optimization, and Recovery》来介绍其对闪存数据保存的分析。

图3-52是闪存基本单元浮栅晶体管的截面图。最上面是控制层，中间是浮栅层，浮栅上面是多晶硅氧化层，下面是隧道氧化层。控制电压很高的时候，会产生量子隧穿效应，电子从衬底Substrate出发，穿过隧道氧化层，进入浮栅保存起来，就完成了写操作。反之，在控制层加很强的负电压，电子就从浮栅量子隧穿，回到衬底，这个操作叫作擦除。不过，控制层不加电压的时候，氧化层依然会产生一个电场，叫作本征电场，它是由浮栅里面的电子产生的。在这个电场的作用下，电子会从浮栅慢慢泄露，泄漏的多了，数据就会发生错误。从写入操作到电子慢慢泄漏，直到数据出错，这个期限叫作数据保存期，在SLC时代，这个时间很久，有好几年，但是到了TLC时代，不到一年，有的只有几个月。

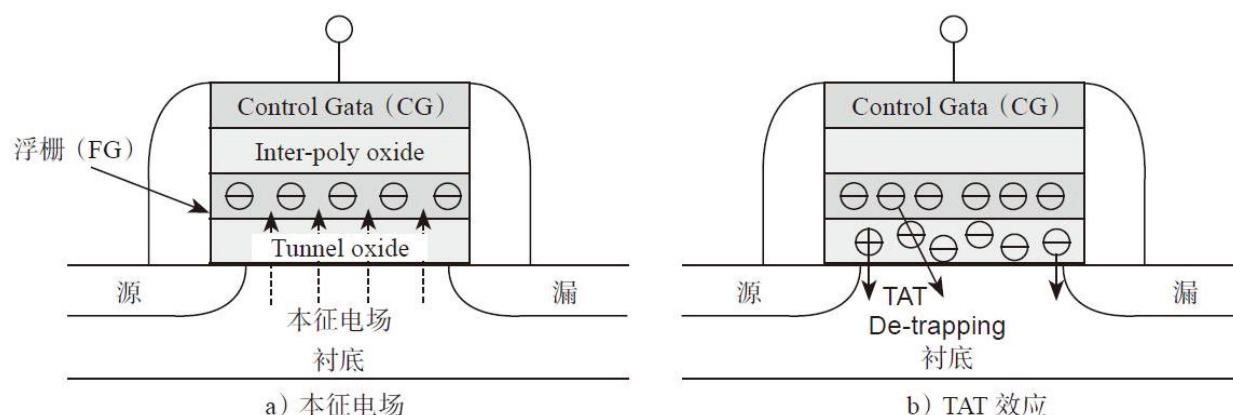


图3-52 浮栅晶体管的本征电场和TAT效应

那为什么闪存用得越久，数据保存时间越短呢？这要怪一个效应：**Trap-assisted tunneling (TAT)**。如图3-54 (b) 所示，我们知道隧道氧化层是绝缘的，但是随着闪存的使用，历经很多次的擦写，氧化层和浮栅层的爱情终于要走到终点了，因为经过这么多年风风雨雨，氧化层老了，有不少通过它的电荷被滞留下来，绝缘体有了导电性。这样，电荷从浮栅跑得就更快了。所以，闪存擦写次数越多，数据保存时间就越短。到最后快到额定擦写次数的时候，比如3000次，刚写的数据就很容易出错。

不过，氧化层并不总是在截留电荷，有时候它拦截的电荷也会离开，叫作**Charge de-trapping**。只不过离开的既有正电荷，也有负电荷，所以对阈值电压的影响是双向的。

那么，怎样解决**Data Retention**的问题呢？总不能让用户的数据放几个月或者几年就丢了吧？一般固态硬盘会采用**Read Scrub**技术，或者叫数据巡检、扫描重写技术等。

如果你对存储技术有所了解，那么当你看到**Scrub**这个词的时候，首先肯定想到的是Sun公司开发的大名鼎鼎的**ZFS (Zettabyte File System)** 文件系统。ZFS的设计者发现，有很多用户的数据长期没有读过，更别说被重写了。即使是数据读取频繁的数据库应用，也存在长期不被访问的数据，它们寂寞地躲在角落里，长期无人问津。但是，不管什么类型的磁盘，总是会有概率发生比特翻转，导致数据出错，等你需要这份数据的时候，错误有可能比较严重，根本恢复不出原样。在ZFS文件系统中，每个数据块都有自己的校验码**Checksum**，只要被读了，就可以通过**Checksum**发现数据是否出错，提前对出错的数

据块进行纠错。所以，ZFS提供了一个功能叫Scrub，对文件系统进行扫描，提前发现那些出错的数据，并纠错重写。

固态硬盘的Read Scrub技术跟ZFS类似，在固态硬盘不忙的时候，按照一定的算法，扫描全盘，如果发现某个闪存页翻转比特数量超过一定阈值，就重写数据到新的地方。这样做的好处是避免数据放太久从而导致比特翻转数量超过ECC算法的纠错能力，这样能减少ECC不可纠错误。

3.4 闪存数据完整性

闪存的一个特性就是随着闪存的使用以及数据存储时间的变长，存储在闪存里面的数据容易发生比特翻转，出现随机性错误。这个问题随着闪存制程的变小越发严重。因此，使用闪存作为存储介质的固态硬盘，需要采用一些数据完整性的技术来确保用户数据可靠不丢失。常见的技术有：

- ECC纠错。
- RAID数据恢复。
- 重读（Read Retry）。
- 扫描重写技术（Read Scrub）。
- 数据随机化。

3.4.1 读错误来源

闪存数据发生错误，主要有以下几个原因：

1. 擦写次数增多

随着闪存块擦写次数增多，氧化层逐渐老化，电子进出存储单元越来越容易，因此存储在存储单元的电荷容易发生异常，导致数据读错误，如图3-53所示。

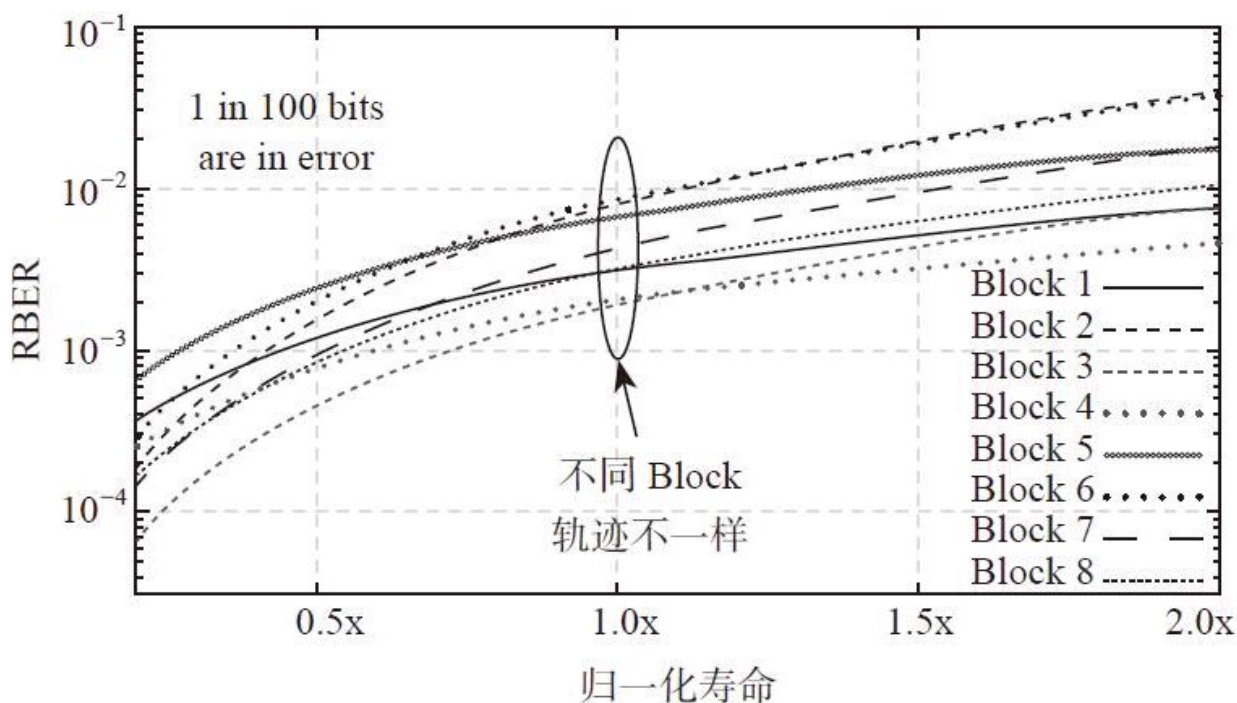


图3-53 同一个闪存芯片内不同闪存块在不同寿命时的RBER

2. Data Retention

随着时间的推移，存储在存储单元的电子会流失，整个阈值电压分布向左移动，导致读数据的时候发生误判，如图3-54所示。

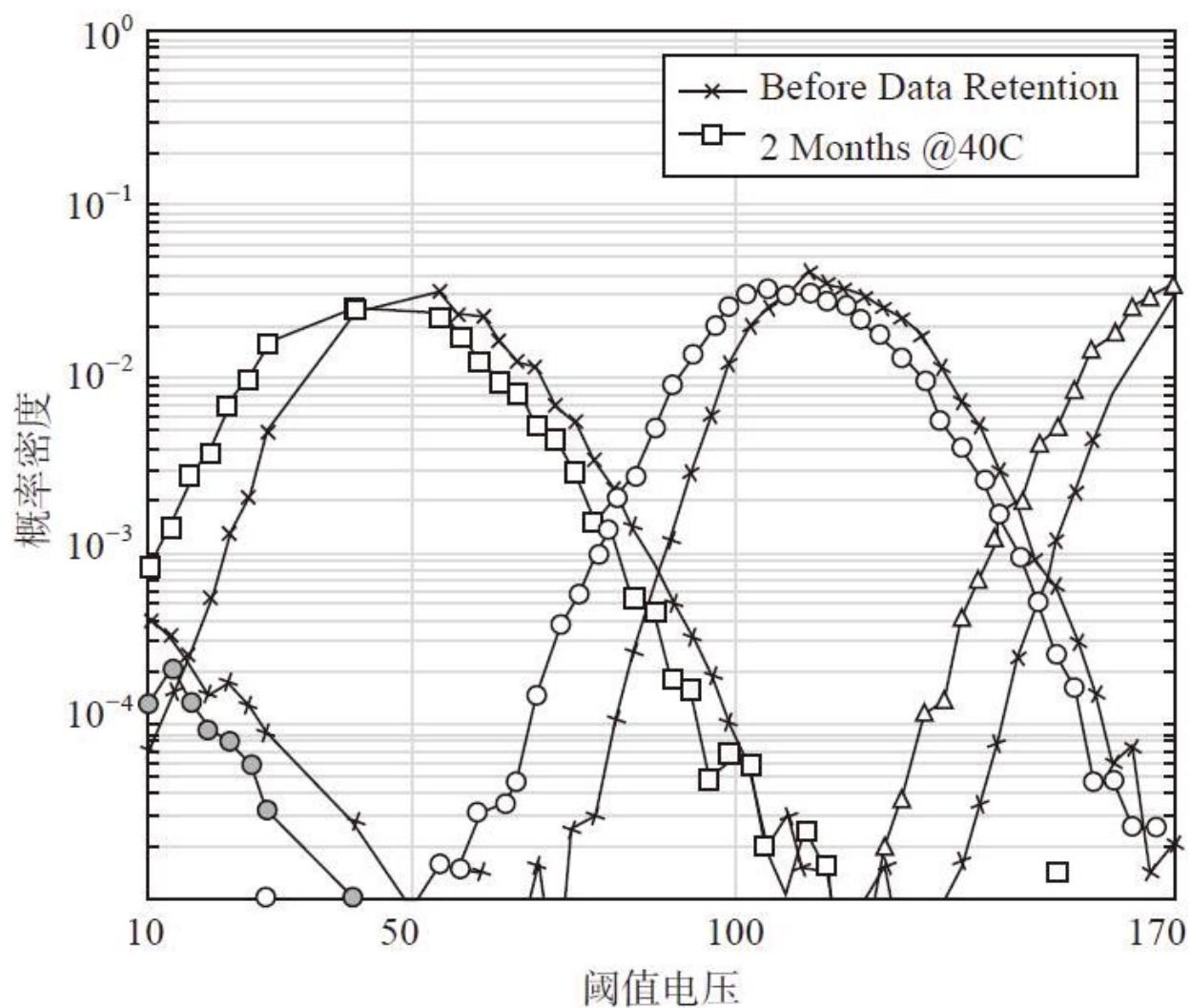


图3-54 阈值电压分布随着时间偏移 [1]

3.读干扰

读一个Wordline数据时，需要施加 V_{pass} 电压在其他Wordline上，导致其他闪存页发生轻微写。如果读的次数过多，轻微写累积起来就会使阈值电压分布发生右移，导致读数据时候发生误判，即读数据错误，如图3-55所示。

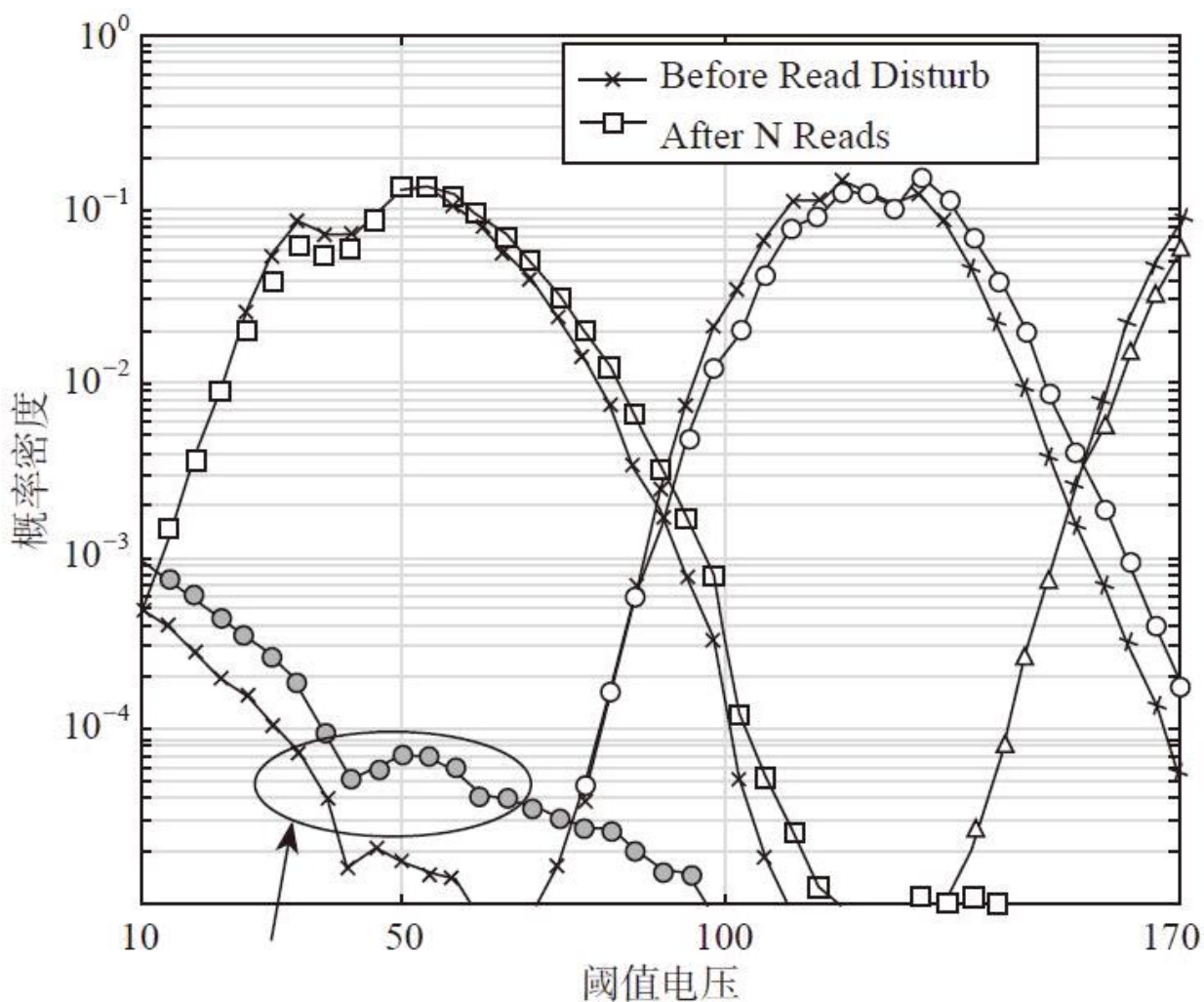


图3-55 读干扰后阈值电压偏移

4. 存储单元之间干扰

由于存储电子的浮栅极是导体，两个导体之间构成电容，一个存储单元电荷的变化会导致其他存储单元电荷变化，而受影响最大的就是与它相邻的存储单元。周围的单元是不同的状态时，中心单元的阈值电压是不一样的，如图3-56所示。

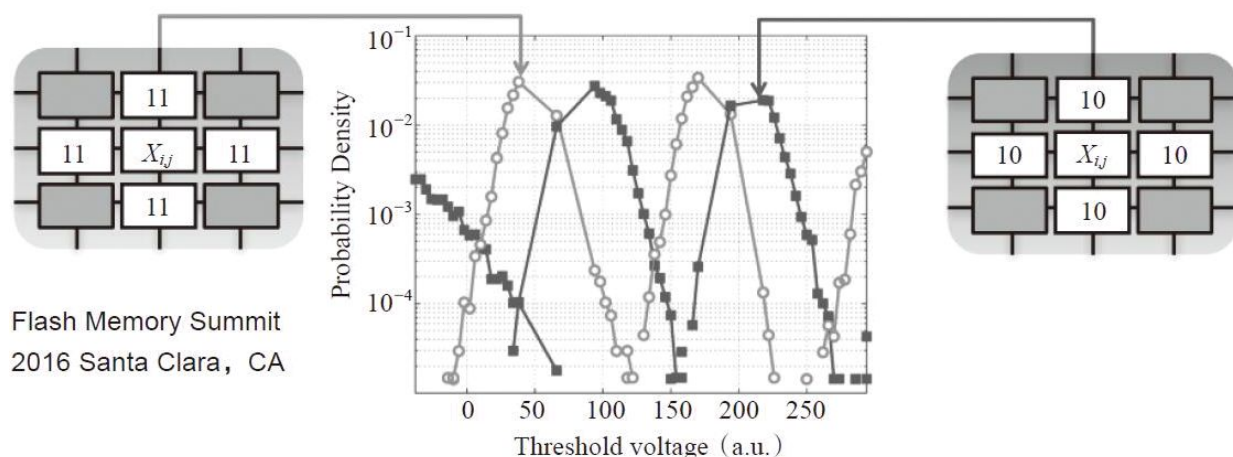


图3-56 周围单元不同状态时的阈值电压分布（来源：FMS 2016）

5.写错误

写错误一般发生在MLC或者TLC 2-pass（先写Lower Page，然后再写Upper Page）写过程中。写Upper Page的时候，它是基于之前Lower Page的状态，然后再写每个存储单元到目标状态。如果写Upper Page的时候，Lower Page数据已经出错（注意写Upper的时候，Lower Page的数据是不会经过控制器ECC纠错的，写过程发生在闪存内部），就会导致存储单元写到一个不期望的状态，即发生写错误。

数据一开始就写错了，当然就别指望读对了。

TLC 1-pass program则没有这个问题，因为Lower Page和Upper Page是一次性同时写入，写Upper Page不依赖于Lower Page数据。当然，如果一开始擦除状态就不对，那么还是会发生写错误。

[1] 本小节图片均来自NAND Flash Basics & Error Characteristics : Thomas Parnell , Roman Pletka IBM Research-Zurich , Flash Memory Summit 2017。

3.4.2 重读

闪存有几种缺陷，对于电压分布平移的问题尚可想办法恢复，因为数据之间还是清楚隔离的。

图3-57以MLC为例，每个存储单元存储两个比特的数据，一共有四种状态。当四种状态的电压分布发生平移后，如果还是采用之前的参考电压去读取的话，就可能会出现读取数据失败的情况。使用重读技术后，我们可以不断改变参考电压，来尝试找到可以读出数据的电压点，直到正确读出数据。理论上，只要这四种状态的电压分布没有发生重叠，就可以通过重读恢复数据。

还有更复杂的重读，叫作Advanced Read Retry。先读附近的单元确定状态，再用不同参考电压读两次要读的单元，根据附近单元数据决定选择哪一个。

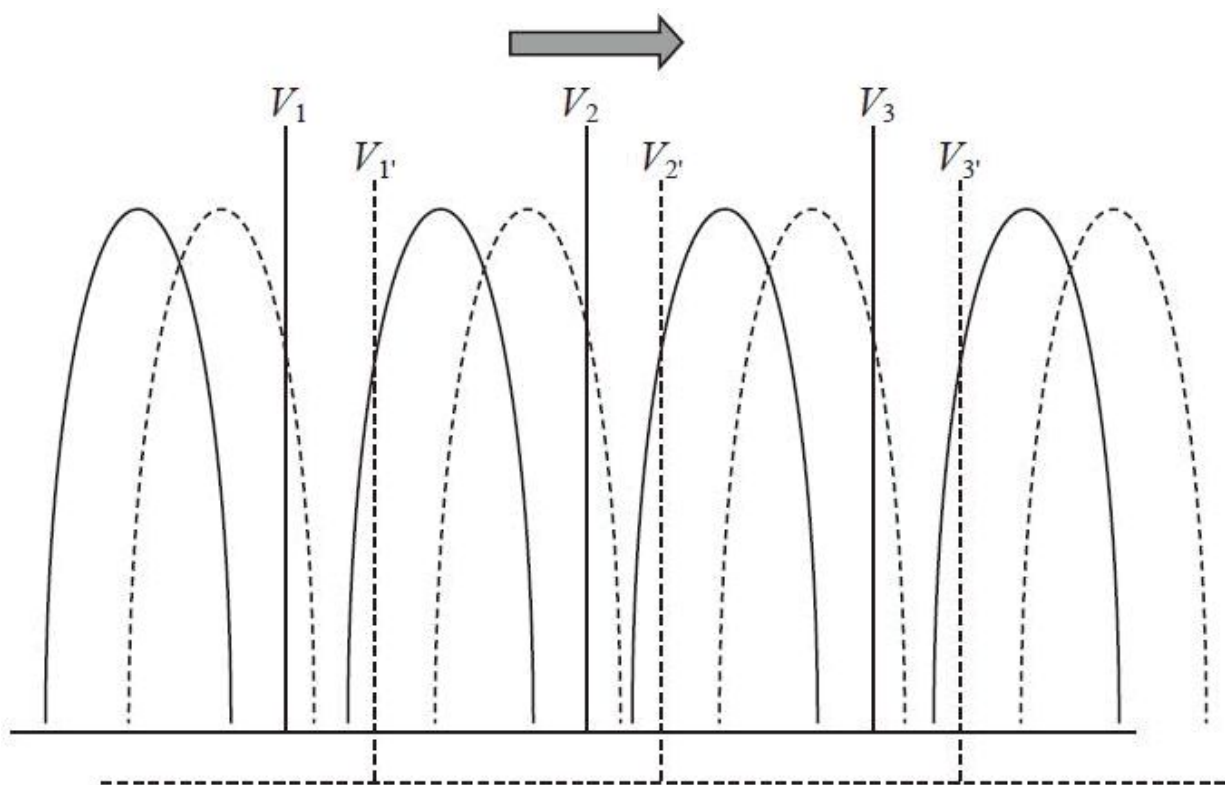


图3-57 平移后电压分布

3.4.3 ECC纠错码

固态硬盘控制器上面都有ECC纠错模块，有些闪存内部也集成了ECC纠错模块。常用闪存ECC纠错算法有BCH（Bose、Ray-Chaudhuri与Hocquenghem三位大神名字的首字母）和LDPC（Low Density Parity Check Code）等。目前市面上很多固态硬盘控制器上采用的是BCH，但采用LDPC正成为一种趋势。

用户数据最终都是写在闪存页（Page）上面，闪存页空间除了用户空间，还有额外的预留空间，这部分空间可以用来写ECC校验数据。用户数据大小固定，需要更强的纠错能力，这就需要更多的ECC空间。因此，纠错强度受限于闪存页的预留空间。越多的预留空间就能提供越强的ECC纠错能力。

目前绝大多数固态硬盘都采用静态ECC纠错方案，ECC纠错单元（用户数据）和ECC校验数据大小在整个固态硬盘生命周期都是固定的，也就是说纠错能力始终保持不变。由于闪存在使用初期内部发生比特翻转的概率小，而随着闪存的使用，出错概率逐渐变大，因此有些固态硬盘开始采用动态ECC纠错方案：开始使用更少的纠错码，这样在闪存的页里面可以存储更多的用户数据；随着固态硬盘的使用，纠错能力需要加强，用户数据在闪存页里面占的比例变小，纠错码所占比例变大。动态ECC纠错方案就是随着固态硬盘的使用，动态调整其ECC纠错能力。动态ECC纠错有什么好处？如果开始使用更少的ECC校验数据，那么每个页能写入的用户数据就更多，相当于固态硬盘拥有更多的OP（Over Provisioning，预留空间），减小了写放大；同时，在数据从控制器写入或者读取闪存的通道上，用户数据越多，ECC校验数据越小，带宽利用率高。

其实，动态ECC的优势不仅体现在随着时间的推移ECC纠错能力会发生变化，而且体现在固态硬盘的闪存位置上每个Die甚至每个闪存页有不同的纠错能力。在固态硬盘闪存阵列里，有些Die可能质量好点，有些Die可能质量差点，好的Die可以用更少的ECC纠错代码；相反，差的Die就需要更强的ECC纠错。对MLC来说，Lower Page相对Upper Page更稳定一些，因此可以使用弱一些的ECC保护；相反，Upper Page则需要更强的ECC保护。

3.4.4 RAID

当闪存中数据比特发生翻转的个数超出ECC纠错能力范围后，ECC纠错就无能为力了。在一些企业级，以及越来越多的消费级固态硬盘上，都在使用RAID（Redundant Arrays of Independent Disks）纠错技术。类似磁盘阵列，固态硬盘内部本质就是一个闪存阵列，所以可以借鉴磁盘阵列技术来确保数据的完整性。固态硬盘的RAID一般采用RAID 5。

以图3-58所示为例，某个固态硬盘的闪存阵列由5个Die构成，Die 0~3存储的是用户数据，Die P则存储校验数据，为Die 0、Die 1、Die 2和Die 3数据之“异或”。假设Die 1上出现ECC不可纠的错误，那么可以通过读取Die 0、Die 2、Die 3和Die P对应位置上的数据，然后做“异或”，就能恢复出Die 1上的数据。

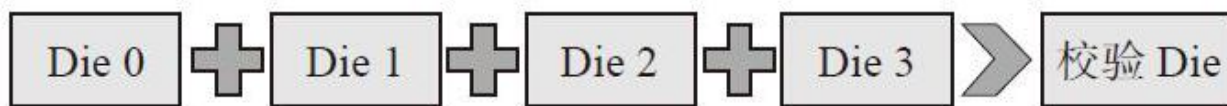


图3-58 RAID 5

采用RAID 5的固态硬盘只能恢复单个ECC不可纠的数据，如果出现多个ECC不可纠的错误，它也无能为力。

由于采用了冗余纠错技术，它需要额外的空间来存储冗余数据（校验数据），因此必然会牺牲用户空间。正应了一句话：天下没有免费的午餐。

看起来容易，做起来难，其实如果你仔细思考一下固态硬盘的写特性就会发现，固态硬盘内部的RAID并不像传统磁盘阵列一样几个硬盘拼成一个组那么简单，需要固态硬盘架构的巨大改变！

如图3-59所示，对传统磁盘RAID 5来说，数据按照条带来写。比如一个磁盘组有4个磁盘，其中一个是校验盘，条带大小为48KB，被拆成三个16KB写到三个盘上，最后一盘是校验数据——三个16KB数据的“异或”值。修改任何一个16KB数据块，都需要重新生成校验数据，并更新校验数据块。

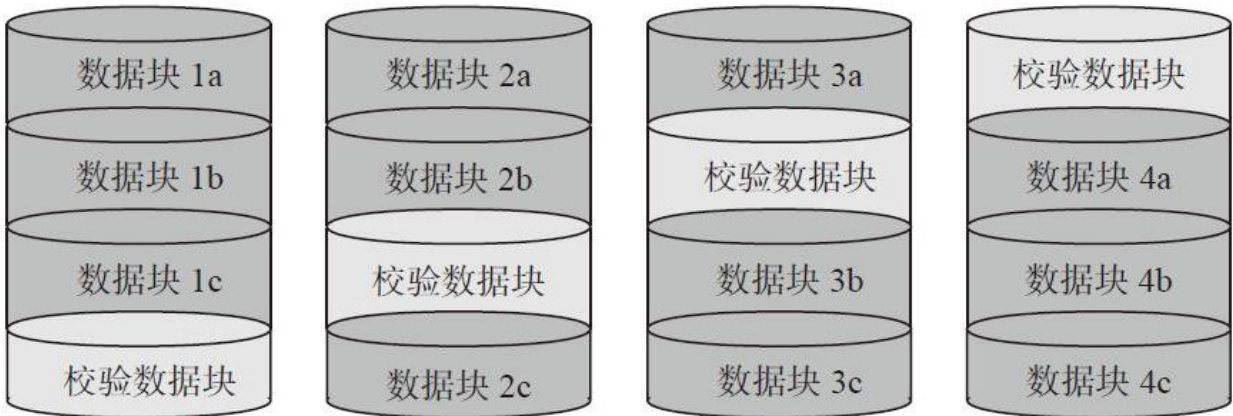


图3-59 传统RAID 5

那么问题来了：固态硬盘可以这么做吗？不行！固态硬盘是不能重写的，每次新写入的数据都会写到新的地方。不过这也没关系，尽管说数据写到了新的地方，但只要旧的数据没有被擦掉，RAID条带还是有效的。

又有了新的问题：条带里面某个Die上的Block被垃圾回收了怎么办？结果是灾难性的，RAID条带失效了。看到这里估计读者朋友也发现了，在固态硬盘里面做RAID最重要的问题就是垃圾回收，要保证整个RAID条带被同时垃圾回收，因为同时被搬走，所以旧的RAID条带也就作废了。

一般固态硬盘内部的RAID是由不同Die上的Block组成的阵列，它们像赤壁之战中曹操的铁索战船一样，绑定在一起：同时被写，同时被垃圾回收，同时被擦除。铁索战船的好处是稳定，缺点是不够灵活。固态硬盘内部的RAID Block船太大了，不太灵活，使得空间被浪费。比如进入休眠之前必须把没写完的条带剩余空间用随机数填满，增加写放大。RAID Block个头大，效率就降低了，有时RAID阵列中某个Block有效数据还很多，但是因为整个阵列有效数据少，不得不整体垃圾回收。世间没有完美的事情，既然选择了稳定的铁索船，那就要承受有一天忽然东南风大作，恰好被黄盖放火烧的风险。

3.4.5 数据随机化

我们在写闪存的时候，如果只是简单地把数据加纠错码写进去，那会遇到很多错误，有时候是写失败，有时候是读出来的数据错误率太高。为什么？因为数据没有随机化。闪存是通过控制栅施加电压来存储数据的，对某些写入的数据样式很敏感，不断地输入全0或者全1，很容易导致闪存内部电量不均衡，从而造成信号抗干扰性下降，导致这些数据在闪存中可靠性变差。

从物理原理上看，闪存写入数据需要做随机化有两个原因：

1) 让0和1的分布充分隔离。图3-60是MLC内部的各个存储状态电压分布图，实线是随机化后的分布，每个状态都充分隔离；虚线是没有随机化的分布，有些状态的分布明显变宽了，随着时间流逝或者寿命缩短，这些分布会和周边发生交集，导致读数据出错。

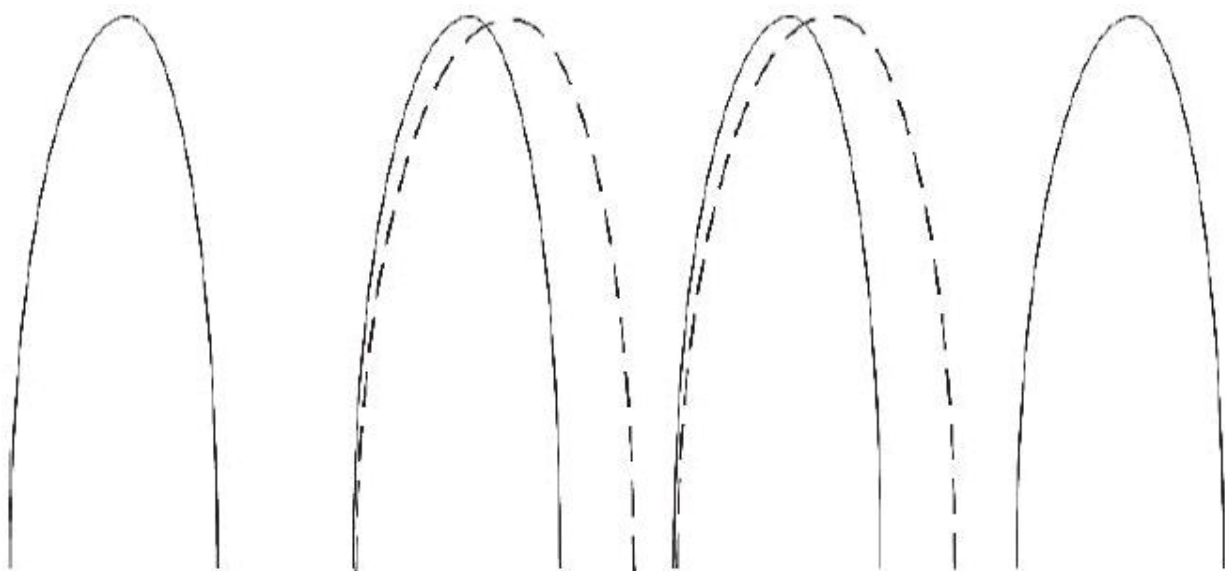


图3-60 没有随机化（虚线）和随机化（实线）电压分布对比

2) 降低相邻单元之间的耦合电压产生的影响。如3-61所示，对一个单元影响最大的是其周围的4个直接相邻的单元，这些单元的状态直接影响到中间单元的阈值电压。

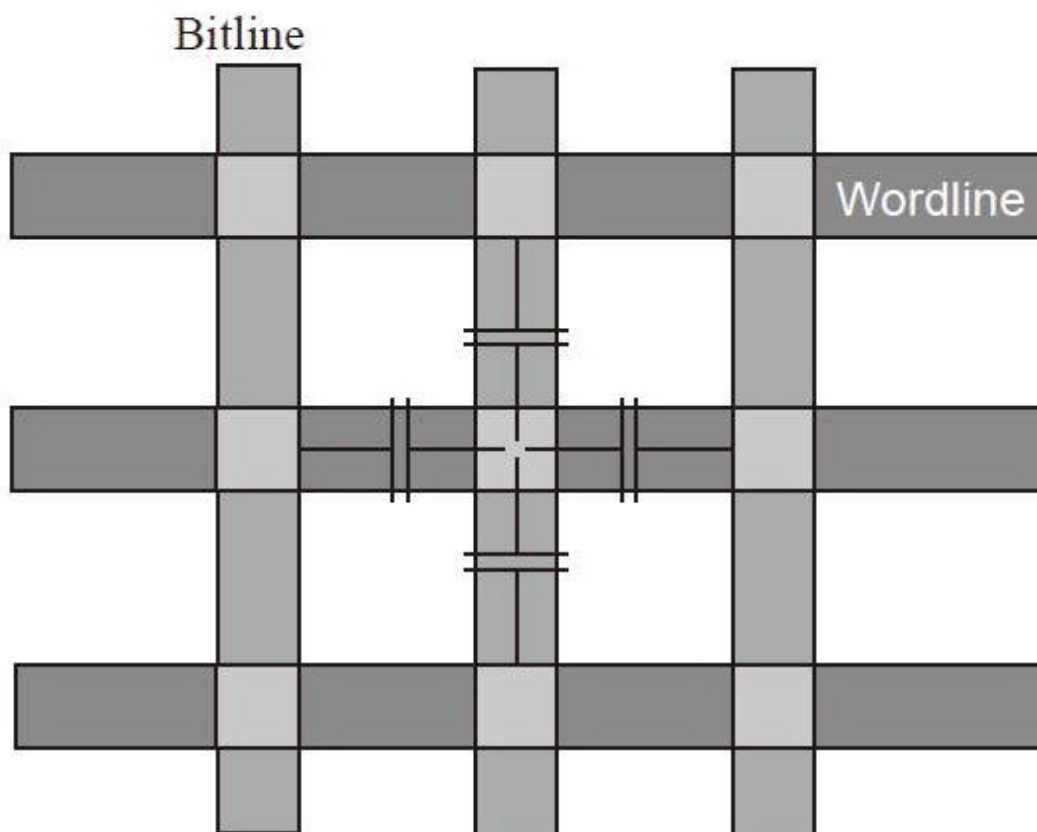


图3-61 周围单元对中心单元的影响

因此，固态硬盘控制器或者闪存内部都有数据随机化模块，它对用户写入的数据加入扰码，使最终写入闪存的数据0和1基本保持均衡，减小数据发生比特翻转的概率。一般闪存厂商会推荐使用AES加密算法实现数据随机化。

那么数据随机化放在哪个位置呢？那自然是在数据最终写到闪存之前，ECC加校验数据之后，数据流如图3-62所示。

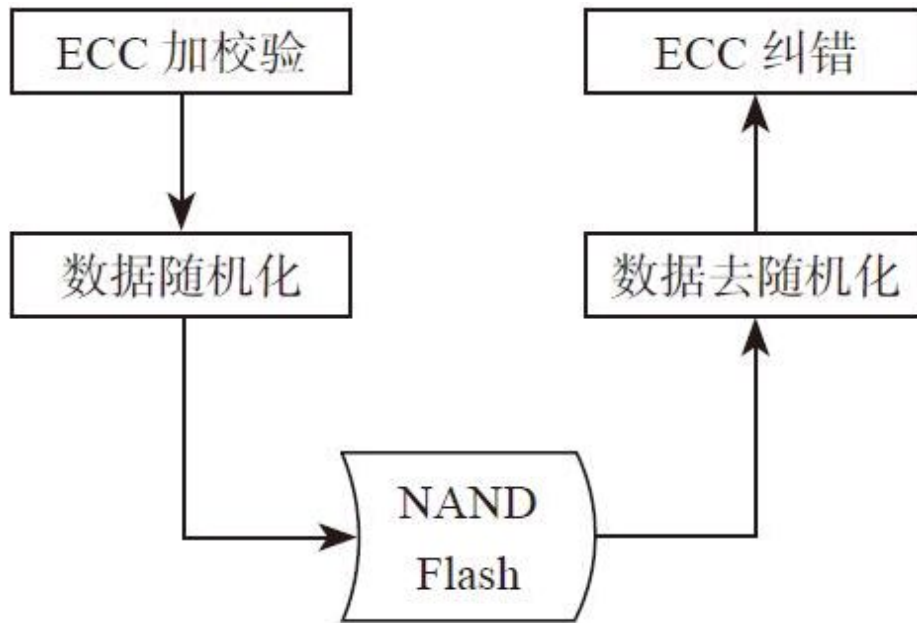


图3-62 数据随机化数据流

在图3-62中，数据随机化也可以在ECC校验之前做，两者顺序可交换。

第4章 SSD核心技术：FTL

4.1 FTL综述

FTL算法的优劣与否，直接决定了SSD在性能（Performance）、可靠性（Reliability）、耐用性（Endurance）等方面的好坏，FTL可以说是SSD固件的核心组成。

那么什么是FTL？FTL是Flash Translation Layer（闪存转换层）的缩写，完成主机（或者用户，Host）逻辑地址空间到闪存（Flash）物理地址空间的翻译（Translation），或者说映射（Mapping）。SSD每把一笔用户逻辑数据写入闪存地址空间，便记录下该逻辑地址到物理地址的映射关系。当主机想读取该数据时，SSD便会根据这个映射，从闪存读取这笔数据然后返回给用户。

完成逻辑地址空间到物理地址空间的映射，这是FTL最原始且基本的功能。事实上，SSD中的FTL还有很多事情可做。SSD使用的存储介质一般是NAND Flash。

SSD的存储介质除了Flash，还有RAM、3D XPoint等新型存储介质。如无特别说明，后文说的SSD存储介质都是指NAND Flash，翻译为NAND闪存，简称闪存。

闪存有一些重要的特性，比如：

1) 闪存块（Block）需先擦除才能写入，不能覆盖写（Update in Place）。

由于闪存块不能覆盖写，当写入一笔新的数据时，不能直接在老地方更改（闪存不允许在一个闪存页（Page）上重复写入，一次擦除只能写入一次），必须写到一个新的位置，因此，FW（FirmWare，固件）需要维护一张逻辑地址到物理地址的映射表。另外，往一个新的位置写入数据，会导致老位置上的数据无效化，这些数据就变为了垃圾数据。垃圾数据会占用闪存空间，当闪存可用空间不够时，FTL需要做垃圾回收，即把若干个闪存块上的有效数据搬出，写到某个新的闪存块，然后把这些之前的闪存块擦除，得到可用的闪存块，这就是GC（Garbage Collection，垃圾回收），是FTL需要做的一件重要的事情。

2) 闪存块都是有一定寿命的。

每擦除一次闪存块，都会对闪存块造成磨损，因此闪存块都是有寿命的，可以用PE（Program/EraseCount）数衡量。我们不能集中往某几个闪存块上写数据，不然这几块很快就会因PE耗尽而死亡，这不是我们想看到的。我们期望所有闪存块都用来均摊数据的写入，而不是有些块飞快磨损，而其他块毫无作为。所以FTL需要做Wear Leveling，让数据写入均摊到每个闪存块上，即让每个块磨损都差不多，从而保证SSD具有最大的数据写入量。

3) 每个闪存块读的次数是有限的，读得太多了，上面的数据便会出错，造成读干扰（Read Disturb）问题。

FTL需要处理读干扰问题，当某个闪存块读的次数将要达到一定阈值时，FTL需要把这些数据从该闪存块上搬走，从而避免数据出错。

4) 闪存的数据保持（Data Retention）问题。

由于电荷的流失，存储在闪存上的数据是会丢失的。这个时间长则十多年，短则几年、几个月，甚至更短（这是在常温下，如果是在高温环境下，电荷流失速度会加快，数据保存的时间就更短了）。

如果SSD不上电，FTL对此也是毫无办法，因为没有运行机会。但一旦上电，FTL就需要对此做点什么，比如扫描闪存，发现是否存在数据保持问题，如果存在，则需要搬动数据，防患于未然。好的FTL，就需要有处理数据保持问题的能力。

5) 闪存天生就有坏块。另外，随着SSD的使用，也会产生新的坏块。

坏块的症状是擦写失败或者读失败（ECC不能纠正数据错误）。坏块管理也是FTL的一大任务。

6) 对MLC或TLC来说，存在Lower Page corruption的问题。

即在对Upper Page/ExtraPage（和Lower Page共享存储单元的闪存页）写入时，如果发生异常掉电，也会把之前Lower Page上成功写入的数据破坏掉。好的FTL，应该有机制尽可能避免这个问题；

7) MLC或TLC的读写速度都不如SLC，但它们都可以配成SLC模式来使用。

好的FTL，会利用该特性去改善SSD的性能和可靠性。

上面说的这些特性是闪存的共性，不同的闪存间还会有各自的问题。FTL除了完成基本的地址映射，还需要处理垃圾回收（GC）、磨损平衡（Wear Leveling）、坏块管理、读干扰（ReadDisturb）处理、数据保持（Data Retention）处理等事情。随着闪存质量变差，FTL除了完成上述常规处理，还需要针对具体闪存特性，去做一些特殊处理以获得好的性能和高的可靠性。

FTL分为Host Based（基于主机）和Device Based（基于设备）。Host Based表示的是，FTL是在Host（主机）端实现的，用的是你自己计算机的CPU和内存资源，如图4-1所示。

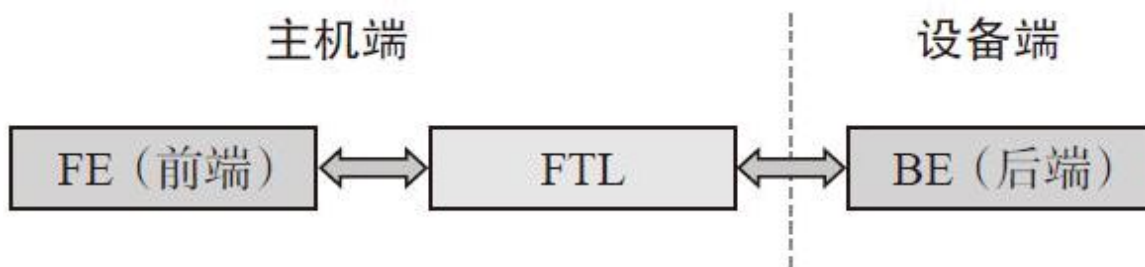


图4-1 FTL在主机端

除了大名鼎鼎的Fusion-IO使用Host Based FTL，业界还有方一信息科技、宝存等公司在做Host Based FTL。

相反，Device Based表示的是，FTL是在Device（设备）端实现的，用的是SSD上的控制器和RAM资源，如图4-2所示。

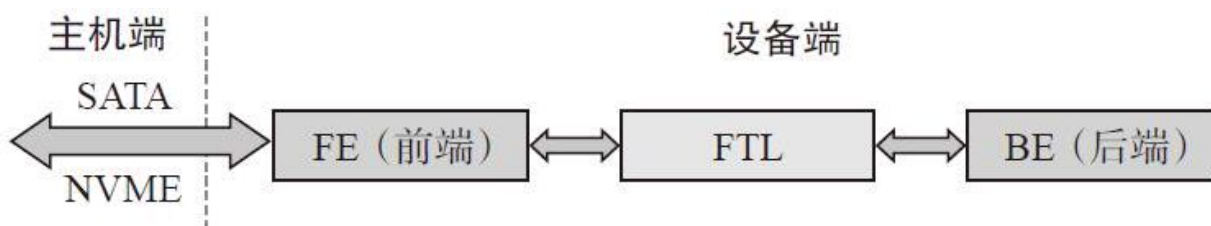


图4-2 FTL在设备端

目前主流SSD都是Device Based FTL，如无特别说明，后文有关FTL的论述都是基于Device Based的。4.10节有关于Host Based FTL的介绍，读者可提前了解。

下面我们来看看FTL的各个关键技术。FTL的初衷是完成逻辑地址（或逻辑空间）到物理地址（或物理空间）的映射，因此我们首先看FTL的映射。

4.2 映射管理

4.2.1 映射种类

根据映射粒度的不同，FTL映射有基于块的映射，有基于页的映射，还有混合映射（Hybrid Mapping）。

块映射中，以闪存的块为映射粒度，一个用户逻辑块可以映射到任意一个闪存物理块，但是映射前后，每个页在块中的偏移保持不变。由于映射表只需存储块的映射，因此存储映射表所需空间小，但其性能差，尤其是小尺寸数据的写入性能，用户即使只写入一个逻辑页，也需要把整个物理块数据先读出来，然后改变那个逻辑页的数据，最后再整个块写入。块映射有好的连续大尺寸的读写性能，但小尺寸数据的写性能是非常糟糕的。

图4-3中，用户空间被划分成一个个逻辑区域（Region），每个区域和闪存块大小相同。

U盘一般都是采用块映射（U盘使用的存储介质也是闪存，因此也是有FTL的），适合大数据的传输，不适合小尺寸数据的写入。所以请不要抱怨U盘随机性能，装系统还是选择SSD吧。

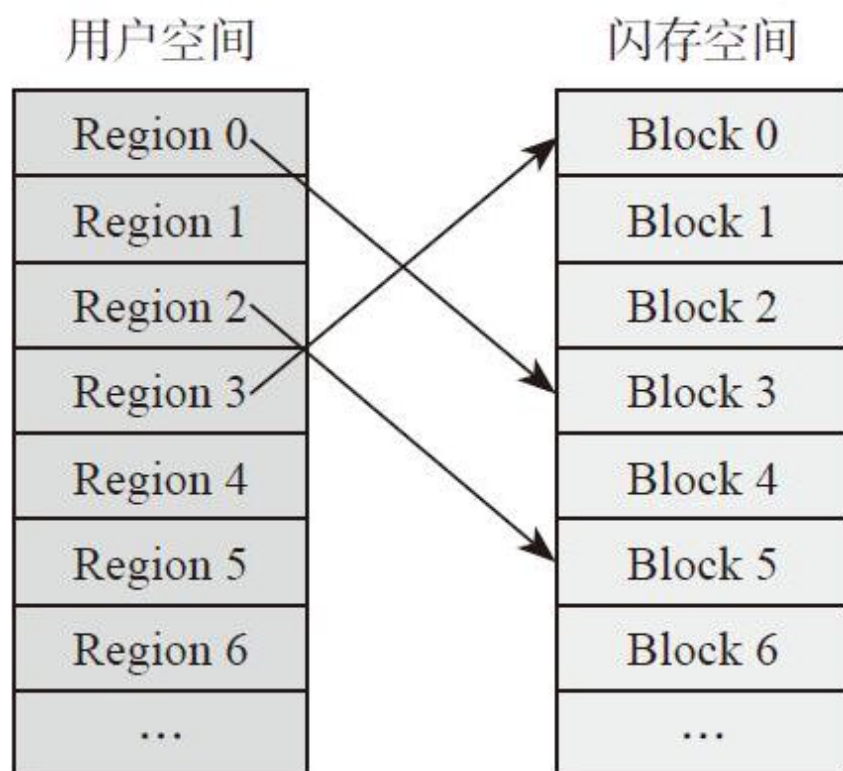


图4-3 块映射

页映射中，以闪存的页为映射粒度，一个逻辑页可以映射到任意一个物理页中，因此每一个页都有一个对应的映射关系，如图4-4所示。由于闪存页远比闪存块多，因此需要更多的空间来存储映射表。但它的性能更好，尤其体现在随机写上面。为追求性能，SSD一般都采用页映射。

图4-4中，用户空间被划分成一个个的逻辑区域，每个区域和闪存页大小相同。

实际中逻辑区域大小可能小于闪存页大小，一个闪存页可容纳若干个逻辑区域数据。

混合映射是块映射和页映射的结合，如图4-5所示。一个逻辑块映射到任意一个物理块，但在块中，每个页的偏移并不是固定不动的，块内采用页映射的方式，一个逻辑块中的逻辑页可以映射到对应物理块中的任意页。因此，它的映射表所需空间以及性能都是介于块映射和页映射之间的。

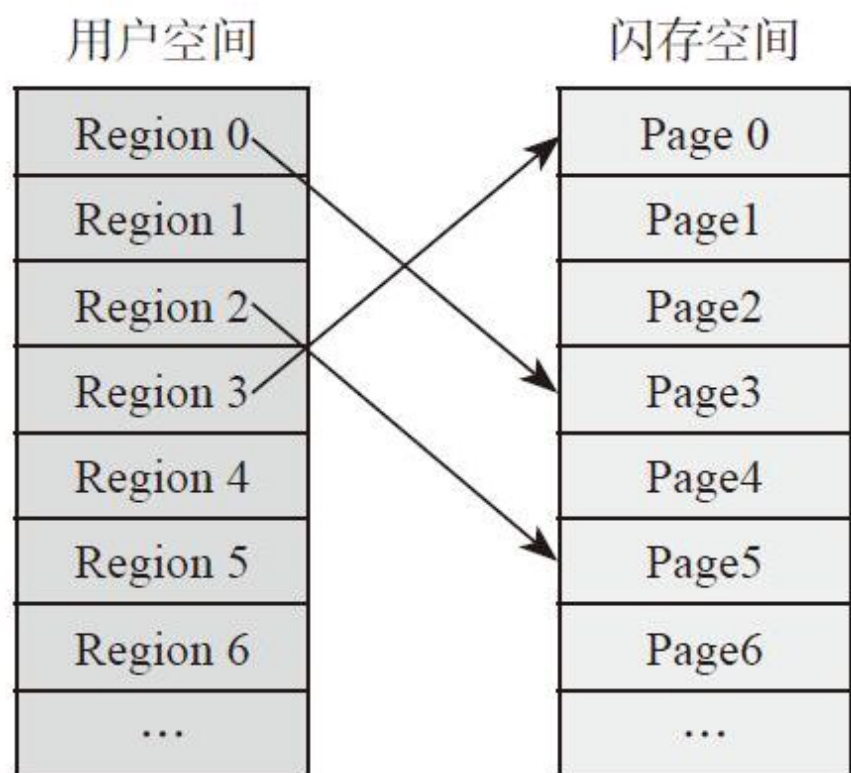


图4-4 页映射

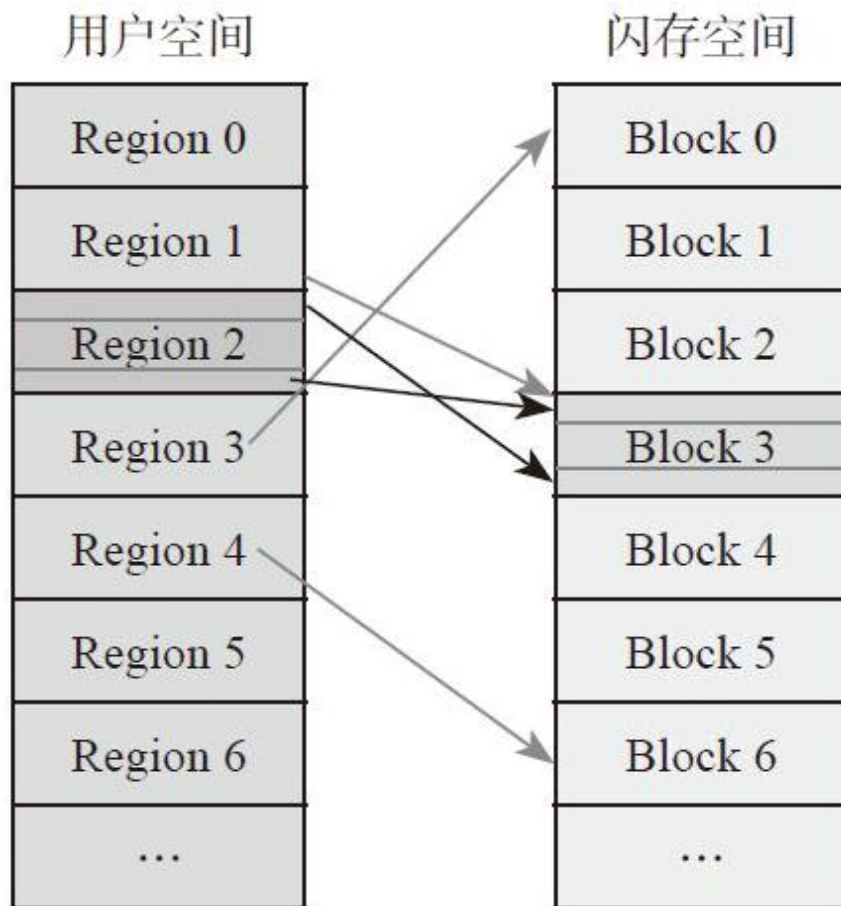


图4-5 混合映射

图4-5中，用户空间划分成一个一个逻辑区域，逻辑区域和闪存块大小相同。每个逻辑块对应着一个闪存块，但逻辑块内部又分成一个个逻辑页，与对应闪存块中的闪存页随意对应。

下面对块映射、页映射和混合映射进行了对比，如表4-1所示。

表4-1 不同映射之间的比较

	块映射	页映射	混合映射
映射单元	物理块	物理页	块页结合
顺序写性能	好	好	好

(续)

	块映射	页映射	混合映射
顺序读性能	好	好	好
随机写性能	很差	好	差
随机读性能	好	好	好
映射表大小	小	大	一般

如无特别说明，我们接下来讲的FTL都是基于页映射的，因为现在SSD基本都是采用这种映射方式。

4.2.2 映射基本原理

用户通过LBA（Logical Block Address，逻辑块地址）访问SSD，每个LBA代表着一个逻辑块（大小一般为512B/4KB/8KB.....），我们把用户访问SSD的基本单元称为逻辑页（Logical Page）。而在SSD内部，SSD主控是以闪存页为基本单元读写闪存的，我们称闪存页为物理页（Physical Page）。用户每写入一个数据页，SSD主控就会找一个物理页把用户数据写入，SSD内部同时记录了这样一条映射（Map）。有了这样一个映射关系后，下次用户需要读某个逻辑页时，SSD就知道从闪存的哪个位置把数据读取上来，如图4-6所示。

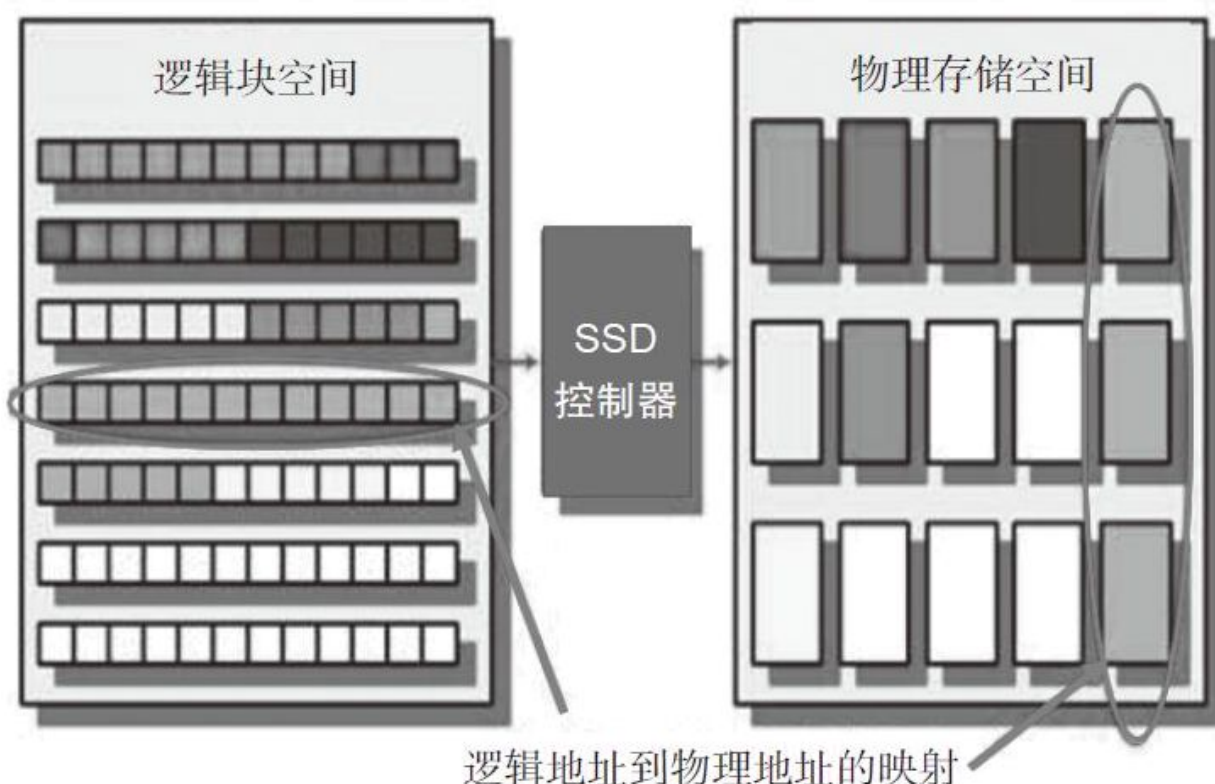


图4-6 逻辑空间到物理空间的映射

SSD内部维护了一张逻辑页到物理页地址转换的映射表（Map Table）。用户每写入一个逻辑页，就会产生一个新的映射关系，这个映射关系会加入（第一次写）或者更改（覆盖写）映射表。当读取某个逻辑页时，SSD首先查找映射表中该逻辑页对应的物理页，然后再访问闪存读取相应的用户数据。

由于闪存页和逻辑页大小不同，一般前者大于后者，所以实际上不会是一个逻辑页对应一个物理页，而是若干个逻辑页写在一个物理页中，逻辑页其实是和子物理页一一对应的。

一张映射表有多大呢？

这里假设我们有一个256GB的SSD，以4KB大小的逻辑页为例，那么用户空间一共有64M（256GB/4KB）个逻辑页，也就意味着SSD需要有能容纳64M条映射关系的映射表。映射表中的每个单元（entry）存储的就是物理地址（Physical Page Address），假设其为4字节（32bits），那么整个映射表的大小为64M×4B=256MB。一般来说，映射表大小为SSD容量大小的千分之一。

准确来说，映射表大小是SSD容量大小的1/1024。前提条件是：映射页大小为4KB，物理地址用4Byte表示。这里假设了SSD内部映射粒度等于逻辑页大小，当然它们可以不一样。

对于绝大多数SSD，我们可以看到上面都有板载DRAM，其主要作用就是存储这张映射表，如图4-7所示。在SSD工作时，全部或绝大部分的映射表都可以放在DRAM上，映射关系可以快速访问。

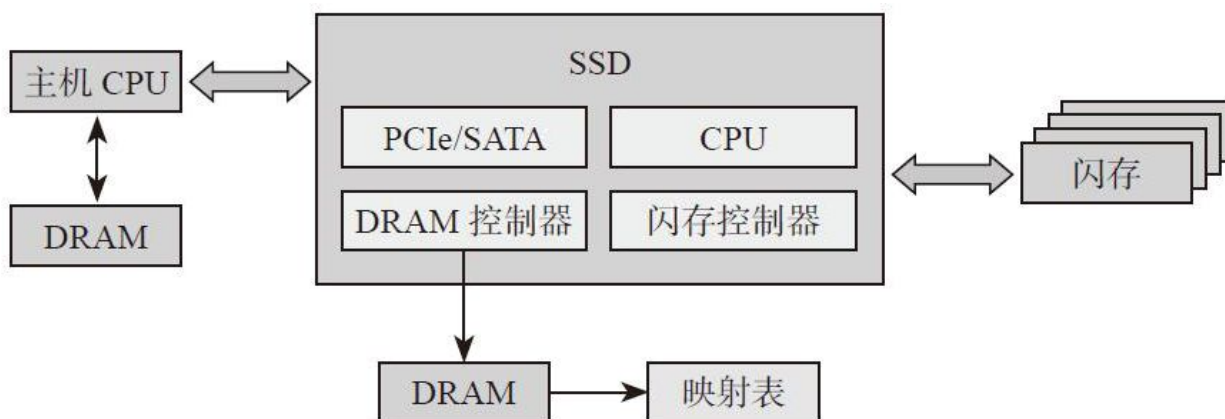


图4-7 带DRAM的SSD架构

但有些入门级SSD或者移动存储设备（比如eMMC、UFS），出于成本和功耗考虑，它们采用DRAM-Less设计，即不带DRAM，比如经典的Sandforce主控，它并不支持板载DRAM，那么它的映射表存在哪里呢？它采用二级映射（见图4-8）。一级映射表常驻SRAM，二级映射表小部分缓存在SRAM，大部分都存放在闪存上。

二级表就是L2P（Logical address To Physical address，逻辑地址到物理地址转换）表，它被分成一块一块（Region）的，大部分存储在闪存中，小部分缓存在RAM中。一级表则存储这些块在闪存中的物理地址，由于它不是很大，一般都可以完全放在RAM中。

SSD工作时，对带DRAM的SSD来说，只需要查找DRAM当中的映射表，获取到物理地址后访问闪存便会得到用户数据，这期间只需要访问一次闪存。而对不带DRAM的SSD来说，它首先会查看该逻辑页对应的映射关系是否在SRAM内：如果在，直接根据映射关系读取闪存；如果不在，那么它首先需把映射关系从闪存中读取出来，然后再根据这个映射关系读取用户数据，这就意味着相比于有DRAM的SSD，它需要读取两次闪存才能把用户数据读取出来，底层有效带宽减小，如图4-9所示。

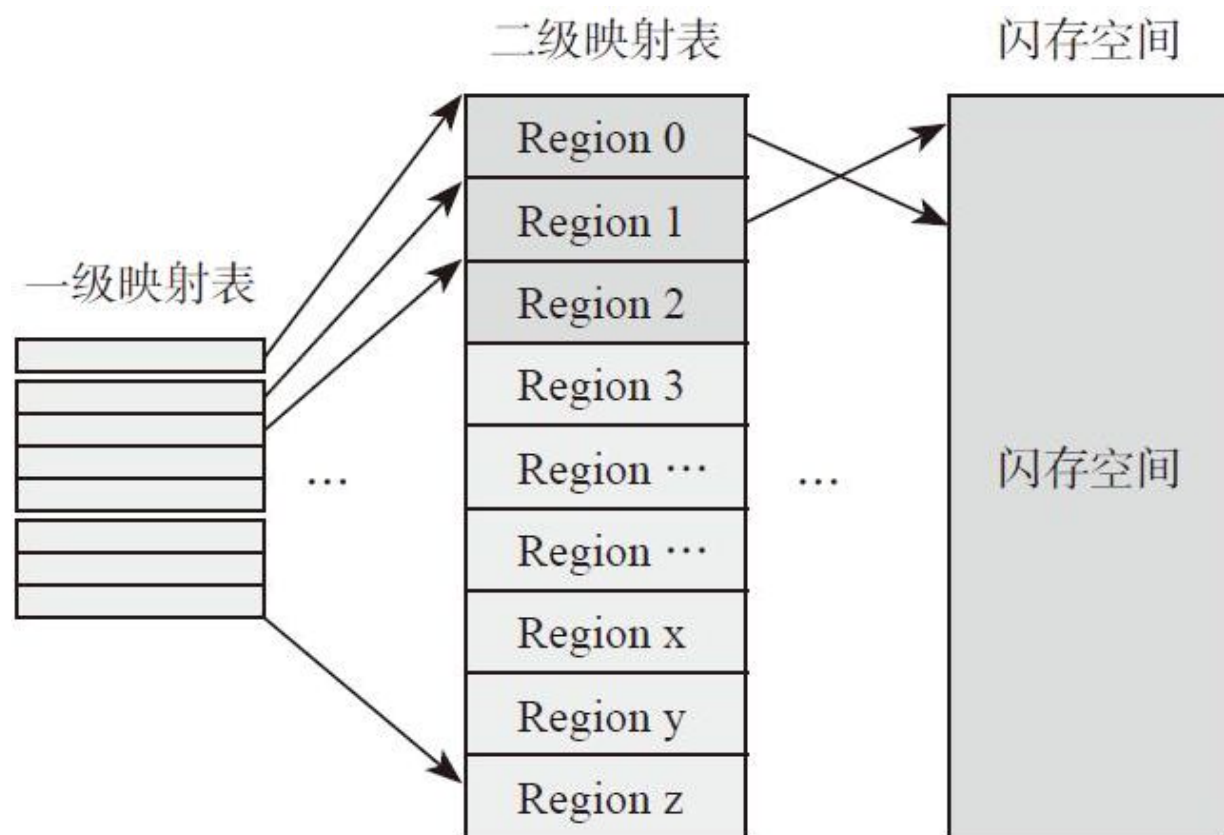


图4-8 两级表映射

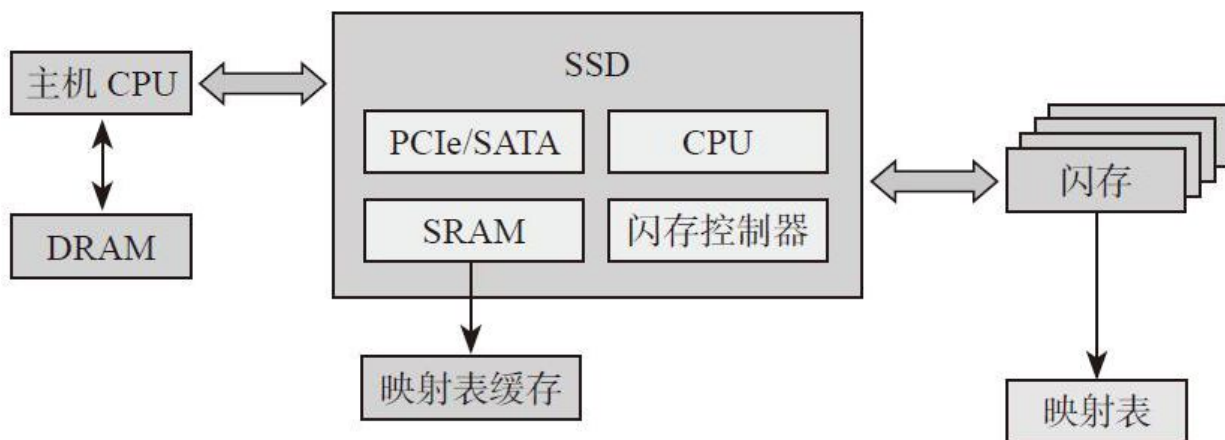


图4-9 不带DRAM的SSD架构

对顺序读来说，映射关系连续，因此一次映射块的读，可以满足很多用户数据的读，也意味着**DRAM-less**的SSD可以有好的顺序读性能。但对随机读来说，映射关系分散，一次映射关系的加载基本只能满足一笔逻辑页的读，因此对随机读来说，需要访问两次闪存才能完成读操作，随机读性能就不是那么理想了。

4.2.3 HMB

映射表除了可以放在板载DRAM、SRAM和闪存中，它还可以放到主机的内存中。NVME1.2（及后续版本）有个重要的功能就是HMB

（Host Memory Buffer，主机高速缓冲存储器）：主机在内存中专门划出一部分空间给SSD用，SSD可以把它当成自己的DRAM使用。因此，映射表完全可以放到主机端的内存中去，如图4-10所示。

在性能上，它应该介于带DRAM和不带DRAM（映射表绝大多数存放在闪存）之间，因为SSD访问主机端DRAM的速度肯定比访问SSD端DRAM的速度要慢，但还是比访问闪存的速度（约40μs）要快。

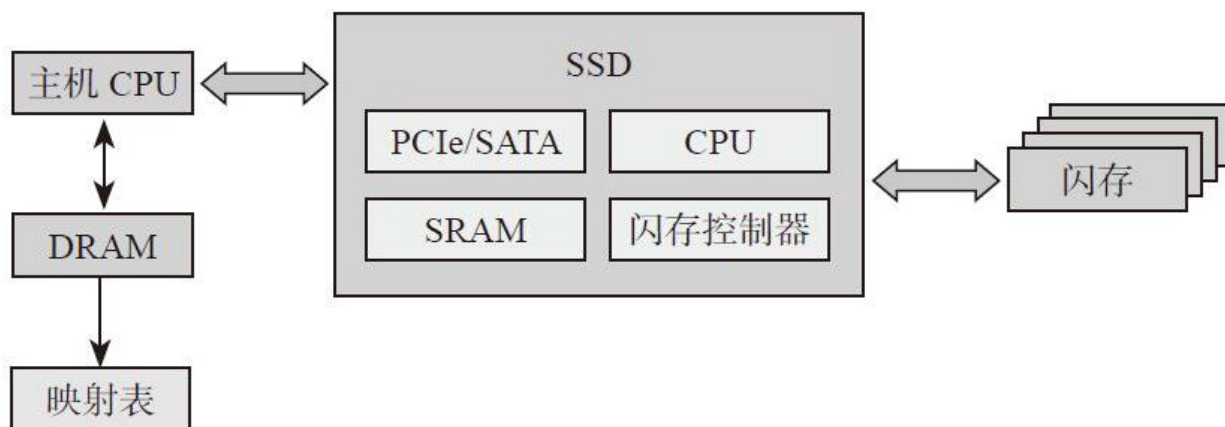


图4-10 基于HMB的SSD架构

Marvell在CES（Consumer Electronics Show）2016上发布了新款SSD主控“88NV1140”，是第一款实现HMB功能的主控。

江波龙2017年发布了目前世界上最小尺寸的SSD（11.5mm×13mm）：P900系列，该产品支持HMB功能。



图4-11 Marvell主控支持HMB

HMB功能允许主控像使用SSD上的DRAM一样使用主机DRAM。具体说来，就是主机在主存中专门划出一块内存给SSD使用，该内存在物理上可以不连续，SSD不仅可以用它来存映射表，还可以用它来缓存用户数据，具体怎么用，取决于SSD设计者。

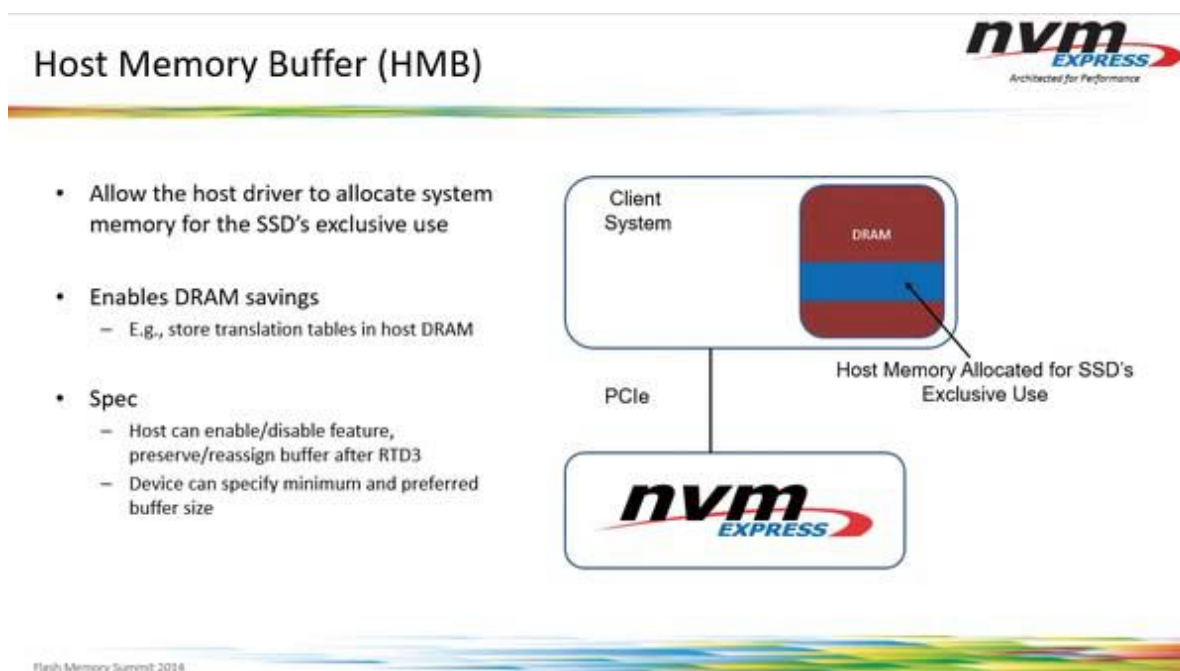


图4-12 HBM介绍

如前所述，SSD有两种设计，一种是带DRAM的，DRAM用于缓存数据和存放映射表，目前主流SSD都是带DRAM的；还有一种就是不带DRAM（DRAM-Less）的，缓存数据用主控上的SRAM，映射表采用两级映射——一级映射和少量的二级映射放SRAM，二级映射数据大多数存放在闪存上，这种DRAM-Less设计多为入门级SSD使用。

带DRAM的SSD设计，其优势是性能好，映射表完全可以放在DRAM上，查找和更新迅速；劣势就是由于增加了一个DRAM，提高了SSD的成本，也加大了SSD的功耗。DRAM-Less的SSD设计则正好相反，优势是成本和功耗相对低，缺点是性能差。由于映射表绝大多数存储在闪存中，对随机读来说，每次读用户数据，需要访问两次闪存，第一次是获取映射表，然后才是真正读取用户数据。

NVMe1.2HMB的出现，以及Marvell新主控对HMB的支持，为SSD的设计提供了新的思路。SSD可以自己不带DRAM，完全用主机DRAM，用以缓存数据和映射表。拿随机读来说，DRAM-Less访问映射表的时间是读闪存的时间。带DRAM的SSD，其访问映射表的时间是读DRAM的时间；而对HMB来说，其访问映射表的时间是访问主机DRAM的时间，接近DRAM SSD，远远短于DRAM-Less SSD或者eMMC、UFS（也是DRAM-Less）。下面是Marvell在2015年闪存峰会上给的一张图（见图4-13，非原图，有改动）。

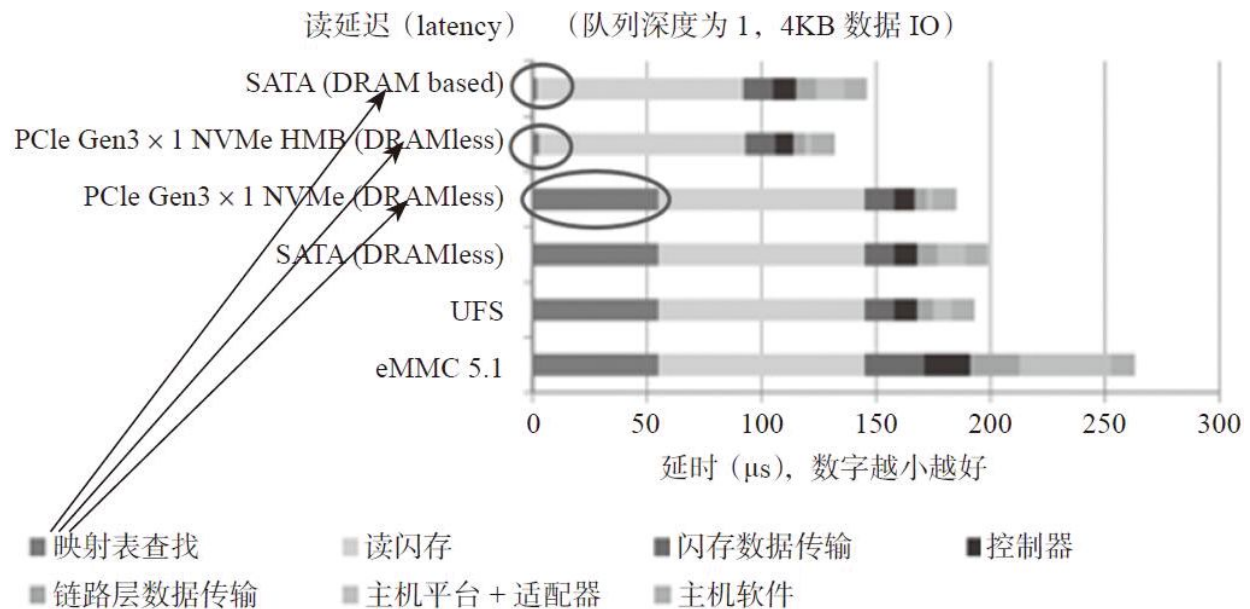


图4-13 不同SSD架构下查询映射表的时延对比

基于HMB的FW实现比较复杂，因为要考虑到即使主机不支持HMB，SSD还要能正常工作。

4.2.4 映射表刷新

映射表在SSD掉电前，是需要把它写入到闪存中去的。下次上电初始化时，需要把它从闪存中部分或全部加载到SSD的缓存（DRAM或者SRAM）中。随着SSD的写入，缓存中的映射表不断增加新的映射关系，为防止异常掉电导致这些新的映射关系丢失，SSD的固件不仅仅只在正常掉电前把这些映射关系刷新到闪存中去，而是在SSD运行过程中，按照一定策略把映射表写进闪存。这样，即使发生异常掉电，丢失的也只是一小部分映射关系，上电时可以较快地重建这些映射关系。

那么，什么时候会触发映射表的写入呢？一般有以下几种情况：

- 新产生的映射关系累积到一定的阈值
- 用户写入的数据量达到一定的阈值
- 闪存写完闪存块的数量达到一定的阈值
- 其他

写入策略一般有：

- 全部更新
- 增量更新

全部更新表示的是缓存中映射表（干净的和不干净的）全部写入到闪存，增量更新的意思是只把新产生的（不干净的）映射关系刷入到闪存中去。显然，相比后者，前者需要写入更多的数据量，一方面影响用户写入性能和时延（latency），另一方面增加写放大，但其好处是固件实现简单，不需要去知道哪些映射关系是干净的，哪些是不干净的。固件算法在决策的时候，应根据软硬件架构，综合考虑，使用最适合自己系统的映射表写入策略。

4.3 垃圾回收

4.3.1 垃圾回收原理

垃圾回收是FTL的一个重要任务。我们虚构一个小小的SSD空间来讲垃圾回收原理，以及与之紧密联系的WA（Write Amplification，写放大）和OP（Over Provisioning，预留空间）等概念。

我们假设该SSD底层有4个通道（CH0～CH3），连接着4个Die（每个通道上的Die可并行操作），假设每个Die只有6个闪存块（Block0～Block5），所以一共24个闪存块。每个闪存块内有9个小方块，每个小方块的大小和逻辑页大小一样。24个闪存块中，我们假设其中的20个闪存块大小为SSD容量，就是主机端看到的SSD大小；另外4个闪存块是超出SSD容量的预留空间，我们称之为OP，如图4-14所示。

好，一个SSD摆在我们面前，下面开始写入了。

我们顺序写入4个逻辑页，分别写到不同通道的Die上，这样写的目的是增加底层的并行性，提升写入性能，如图4-15所示。

我们继续顺序写入，固件则把数据交错写入到各个Die上，直到写满整个SSD空间（主机端看到的）如图4-16所示。

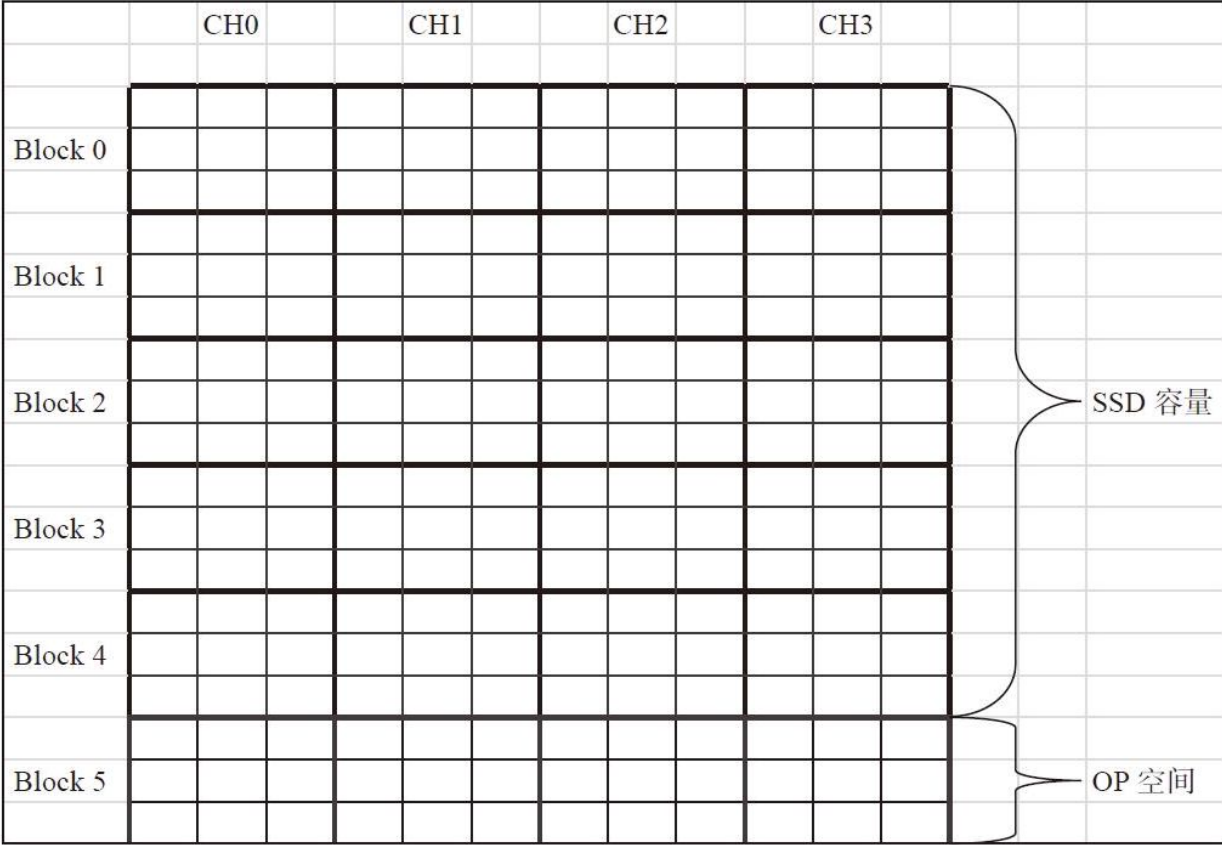


图4-14 虚构的小小SSD空间

	CH0			CH1			CH2			CH3		
	1			2			3			4		
Block 0												
Block 1												
Block 2												
Block 3												
Block 4												
Block 5												

图4-15 主机写入4个逻辑页数据后

	CH0			CH1			CH2			CH3		
	1	5	9	2	6	10	3	7	11	4	8	12
Block 0	13	17	21	14	18	22	15	19	23	16	20	24
	25	29	33	26	30	34	27	31	35	28	32	36
	37	41	45	38	42	46	39	43	47	40	44	48
Block 1	49	53	57	50	54	58	51	55	59	52	56	60
	61	65	69	62	66	70	63	67	71	64	68	72
	73	77	81	74	78	82	75	79	83	76	80	84
Block 2	85	89	93	86	90	94	87	91	95	88	92	96
	97	101	105	98	102	106	99	103	107	100	104	108
	109	113	117	110	114	118	111	115	119	112	116	120
Block 3	121	125	129	122	126	130	123	127	131	124	128	132
	133	137	141	134	138	142	135	139	143	136	140	144
	145	149	153	146	150	154	147	151	155	148	152	156
Block 4	157	161	165	158	162	166	159	163	167	160	164	168
	169	173	177	170	174	178	171	175	179	172	176	180
Block 5												

图4-16 用户空间写满后的SSD

整个盘写满了（从用户角度来看也就是整个用户空间写满了，但在闪存空间，由于OP的存在，并没有写满）。那如果想写入更多，应该怎么办？别无他法，只能把看过的内容割爱删除了，腾出空间放新的内容。

下面我们继续拷入。

假设还是从逻辑页1开始写入。这时，SSD会把新写入的逻辑页写入到所谓的OP空间。对SSD来说，不存在什么用户空间和OP空间，它只会看到闪存空间。主机端来数据，SSD就往闪存空间写。图4-17中出现了深色方块，怎么回事？因为逻辑页1~4的数据已更新，写到新的地方，那么之前那个位置上的逻辑页1~4数据就失效了，过期了，变

垃圾了。用户更新数据，由于闪存不能在原位置覆盖写，固件只能另找闪存空间写入新的数据，因此导致原闪存空间数据过期，形成垃圾。

继续顺序写入，深色方块越来越多（垃圾数据越来越多）。所有闪存空间都写满后，小SSD就是下面这个样子（见图4-18）。

等所有Die上的Block 5写满后，所有Die上的Block 0也全部变色了（这些数据都是垃圾）。

现在不仅整个用户空间都写满，整个闪存空间也都满了。如果用户想继续写入后续的逻辑页（36之后的），该怎么办呢？

这时，就需要垃圾回收了。我们暂时从之前的SSD系统中走出来，看看什么是垃圾回收。

	CH0			CH1			CH2			CH3		
	1	5	9	2	6	10	3	7	11	4	8	12
Block 0	13	17	21	14	18	22	15	19	23	16	20	24
	25	29	33	26	30	34	27	31	35	28	32	36
	37	41	45	38	42	46	39	43	47	40	44	48
Block 1	49	53	57	50	54	58	51	55	59	52	56	60
	61	65	69	62	66	70	63	67	71	64	68	72
	73	77	81	74	78	82	75	79	83	76	80	84
Block 2	85	89	93	86	90	94	87	91	95	88	92	96
	97	101	105	98	102	106	99	103	107	100	104	108
	109	113	117	110	114	118	111	115	119	112	116	120
Block 3	121	125	129	122	126	130	123	127	131	124	128	132
	133	137	141	134	138	142	135	139	143	136	140	144
	145	149	153	146	150	154	147	151	155	148	152	156
Block 4	157	161	165	158	162	166	159	163	167	160	164	168
	169	173	177	170	174	178	171	175	179	172	176	180
	1			2			3			4		
Block 5												

图4-17 删除4个逻辑页后再次写入4个逻辑页

		CH0				CH1				CH2				CH3			
		1	5	9	2	6	10	3	7	11	4	8	12				
Block 0		13	17	21	14	18	22	15	19	23	16	20	24				
		25	29	33	26	30	34	27	31	35	28	32	36				
		37	41	45	38	42	46	39	43	47	40	44	48				
Block 1		49	53	57	50	54	58	51	55	59	52	56	60				
		61	65	69	62	66	70	63	67	71	64	68	72				
		73	77	81	74	78	82	75	79	83	76	80	84				
Block 2		85	89	93	86	90	94	87	91	95	88	92	96				
		97	101	105	98	102	106	99	103	107	100	104	108				
		109	113	117	110	114	118	111	115	119	112	116	120				
Block 3		121	125	129	122	126	130	123	127	131	124	128	132				
		133	137	141	134	138	142	135	139	143	136	140	144				
		145	149	153	146	150	154	147	151	155	148	152	156				
Block 4		157	161	165	158	162	166	159	163	167	160	164	168				
		169	173	177	170	174	178	171	175	179	172	176	180				
		1	5	9	2	6	10	3	7	11	4	8	12				
Block 5		13	17	21	14	18	22	15	19	23	16	20	24				
		25	29	33	26	30	34	27	31	35	28	32	36				

图4-18 闪存空间写满

需要说明的是，实际中是不会等所有闪存空间都写满后才开始做GC的，而是在满之前就触发GC，这里只是为描述GC而做的假设。

垃圾回收，就是把某个闪存块上的有效数据（图4-19中浅色方块）读出来，重写，然后把该闪存块擦除，就得到新的可用闪存块了。

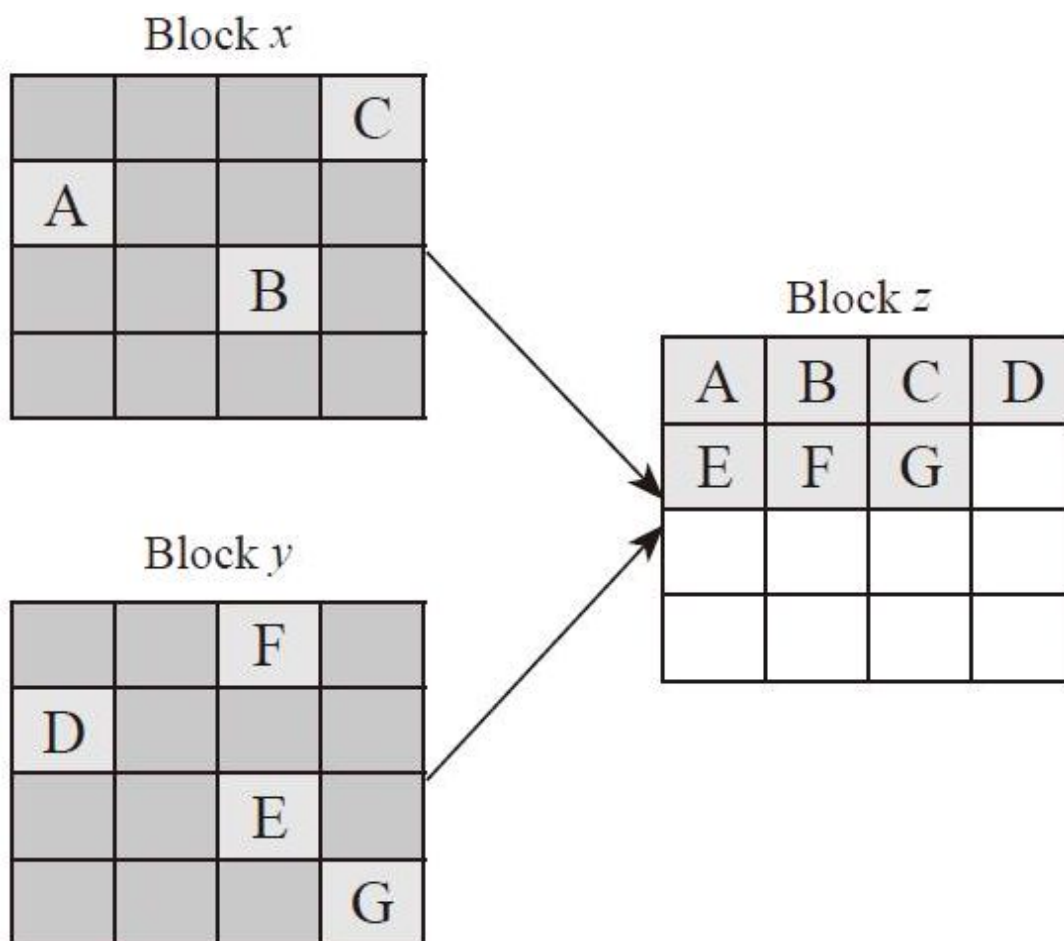


图4-19 垃圾回收示例

图4-19中，Block x上面有效数据为A、B、C，Block y上面有效数据为D、E、F、G，其余方块为无效数据。垃圾回收机制就是先找一个可用Block z，然后把Block x和Block y的有效数据搬移到Block z上面去，这样Block x和Block y上面就没有任何有效数据，可以擦除变成两个可用的闪存块，如图4-20所示。

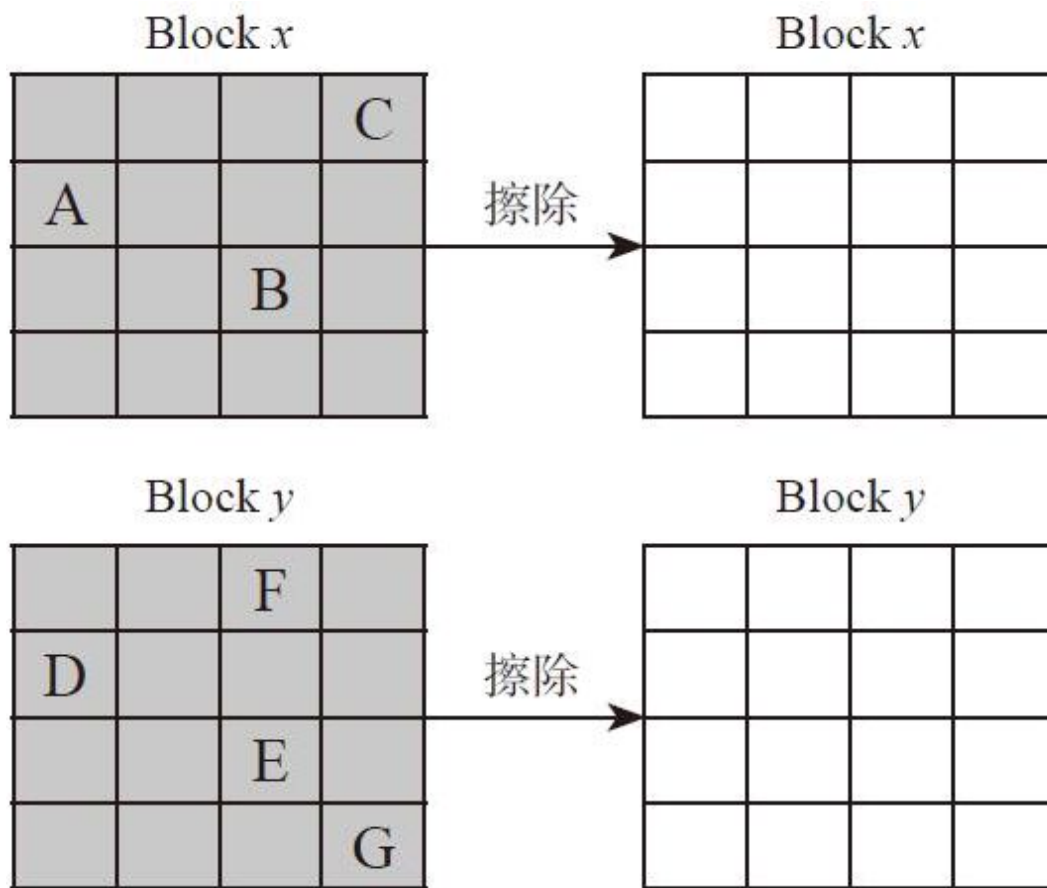


图4-20 擦除垃圾数据块变成可用数据块

再回到我们的小小SSD系统中来。

上例中，由于我们是顺序写入，垃圾集中在Block 0上，上面没有任何有效数据，我们把它们擦除就可以腾出新的写入空间，用户就可以把新的数据写入到垃圾回收完成的Block 0上了。从这个例子中我们可以看出：顺序写，即使是闪存空间写满后的写（Full Drive写），性能也是比较好的，因为垃圾回收可以很快完成（也许只需要一个擦除动作）。

但现实是残酷的：用户写入数据，更多的可能是随机写入数据。下面是一个闪存空间经历随机写满后的样子（见图4-21）。

	CH0			CH1			CH2			CH3		
Block 0	154	108	121	46	11	110	37	110	157	134	73	31
	123	19	131	6	45	173	54	35	71	165	96	141
	164	134	57	109	172	86	158	59	107	109	118	34
Block 1	10	54	135	68	90	10	150	100	22	167	126	119
	104	98	63	85	46	94	148	123	7	17	176	59
	27	22	118	50	51	28	91	40	110	3	161	103
Block 2	57	3	115	21	114	144	157	98	54	132	71	24
	76	48	83	111	106	120	54	34	179	152	47	106
	26	1	106	179	137	112	6	38	107	20	167	49
Block 3	17	84	177	155	3	149	172	160	80	52	20	57
	45	78	141	141	70	37	178	66	56	61	119	163
	106	135	43	55	93	166	172	103	44	164	119	150
Block 4	172	132	3	150	79	173	148	172	11	133	175	68
	34	118	169	34	2	162	16	156	66	30	79	117
	8	12	90	92	22	88	153	81	83	53	13	26
Block 5	20	157	106	180	155	131	82	53	59	72	26	1
	14	132	20	151	82	128	77	168	9	113	111	22
	96	175	111	83	28	60	178	126	22	166	135	9

图4-21 随机写满闪存空间后的SSD

用户如果继续往SSD上写入数据，那么SSD怎么处理？当然需要做垃圾回收。不过，SSD内部状况比之前看到的复杂多了，垃圾数据分散在每个闪存块上，而不是集中在某几个闪存块上。这个时候，如何挑选需要回收的闪存块呢？答案显而易见，挑垃圾比较多的闪存块来回收，因为有效数据少，要搬移的数据少，这样腾出空闪存块的速度快。

对上面每个闪存块的垃圾数（深色方块）做个统计，如表4-2所示。

表4-2 每个闪存块上垃圾数据统计

	CH 0	CH 1	CH 2	CH 3	垃圾总数
BLOCK 0	4	8	7	5	24
BLOCK 1	5	3	3	7	19
BLOCK 2	6	2	4	3	15
BLOCK 3	3	3	4	3	13
BLOCK 4	3	2	1	3	9
BLOCK 5	1	0	2	2	5

由于是同时往4个通道上写，我们需要每个通道都有一个空闲的闪存块，因此，我们做垃圾回收时，不是回收某个闪存块，而是所有通道上都要挑一个。一般选择每个Die上块号一样的所有闪存块做垃圾回收。上例中，Block 0上的垃圾数量最多（24个深色方块，最多），因此我们挑Block 0作为垃圾回收的闪存块（这里忽略PE Count等因素，只看垃圾数）。回收完毕，我们把之前Block 0上面的有效数据（浅色方块）重新写回到这些闪存块（这里，我们假设回收的有效数据和用户数据写在同一个闪存块，实际上，它们可能是分开写的），如图4-22所示。

	CH0			CH1			CH2			CH3		
Block 0	154	31	134	108	19	86	121	35	158	73	165	109
Block 1	10	54	135	68	90	10	150	100	22	167	126	119
	104	98	63	85	46	94	148	123	7	17	176	59
	27	22	118	50	51	28	91	40	110	3	161	103
Block 2	57	3	115	21	114	144	157	98	54	132	71	24
	76	48	83	111	106	120	54	34	179	152	47	106
	26	1	106	179	137	112	6	38	107	20	167	49
Block 3	17	84	177	155	3	149	172	160	80	52	20	57
	45	78	141	141	70	37	178	66	56	61	119	163
	106	135	43	55	93	166	172	103	44	164	119	150
Block 4	172	132	3	150	79	173	148	172	11	133	175	68
	34	118	169	34	2	162	16	156	66	30	79	117
	8	12	90	92	22	88	153	81	83	53	13	26
Block 5	20	157	106	180	155	131	82	53	59	72	26	1
	14	132	20	151	82	128	77	168	9	113	111	22
	96	175	111	83	28	60	178	126	22	166	135	9

图4-22 做完垃圾回收后的Block 0可以继续写入数据

这时，有了空闲的空间（白色方块），用户就可以继续写入数据了。

江湖传言：**SSD**越写越慢。没错，其实这是有科学依据的：可用闪存空间富裕时，**SSD**是无须做**GC**的，因为总有空闲的空间可写。**SSD**使用早期，由于没有触发**GC**，无须额外的读写，所以速度很快。慢慢地会发现**SSD**变慢了，主要是因为**SSD**需要做**GC**。

另外，从上面的例子来看，如果用户顺序写的话，垃圾比较集中，利于**SSD**做垃圾回收；如果用户是随机写的话，垃圾产生比较分散，**SSD**做垃圾回收相对来说就更慢，所以性能没有前者好。因此，

SSD的GC性能跟用户写入数据的模式（随机写还是顺序写）也是有关的。

4.3.2 写放大

由于GC的存在，就有一个问题，用户要写入一定的数据，SSD为了腾出空间写这些数据，需要额外的做一些数据的搬移，也就是额外的写，最后往往导致SSD往闪存中写入的数据量比实际用户写入SSD的数据量多。因此，SSD中有个重要参数，就是写放大（WA，Write Amplification）：

$$\text{写放大} = \frac{\text{写入闪存的数据量}}{\text{用户写的数据量}}$$

对空盘来说（未触发GC），写放大一般为1，即用户写入多少数据，SSD写入闪存也是多少数据量（这里忽略SSD内部数据的写，如映射表的写入）。在SandForce控制器出来之前，写放大最小值为1。但是由于SandForce控制器内部具有实时数据压缩模块，它可对用户写入的数据进行实时压缩，然后再把它们写入到闪存，因此WA可以做到小于1。举个例子，用户写入8KB数据，经压缩后，数据变为4KB，如果这个时候还没有垃圾回收，那么写放大就只有0.5。

来看看GC触发后，WA是怎么算的。以前面的GC为例，我们挑选每个Die上的Block 0做垃圾回收，如图4-23所示。

	CH0			CH1			CH2			CH3		
Block 0	154	108	121	46	11	110	37	110	157	134	73	31
	123	19	131	6	45	173	54	35	71	165	96	141
	164	134	57	109	172	86	158	59	107	109	118	34

图4-23 Block 0数据示意

一共36个方块，其中有12个有效数据块，我们做完垃圾回收后，需把这12个有效数据块写回，如图4-24所示。

	CH0			CH1			CH2			CH3		
Block 0	154	31	134	108	19	86	121	35	158	73	165	109

图4-24 垃圾回收后，将有效数据写回Block 0

后面还可以写入24个方块的用户数据。因此，为了写这24个方块的用户数据，SSD实际写了12个方块的原有效数据，再加上该24个方块的用户数据，总共写入36个方块数据，按照写放大定义：
 $WA=36/24=1.5$ 。

写放大越大，意味着额外写入闪存的数据越多，一方面磨损闪存，减少SSD寿命，另一方面，写入这些额外数据会占用底层闪存带宽，影响SSD性能。因此，SSD设计的一个目标是让WA尽量小。减小写放大，可以使用前面提到的压缩办法（主控决定），顺序写也可以减小写放大（垃圾集中，但顺序写可遇不可求，取决于用户Workload），还有就是增大OP（这个可控）。

增大OP为何能减小写放大？先定义OP比例=（闪存空间-用户空间）/用户空间。

还是以前面的SSD空间为例，SSD容量是180个小方块，当OP是36个小方块时，整个SSD闪存空间为216个小方块，OP比例是 $36/180=20\%$ 。那么180个小方块的用户数据平均分摊到216个小方块时，每个小方块的平均有效数据为 $180/216=0.83$ ，一个闪存块上的有效数据为 $0.83 \times 9=7.5$ ，也就是一个闪存块上面平均有7.5个浅色块和1.5个深色块。为了写1.5个用户数据方块，需要写9个方块的数据（原有7.5个有效数据，加1.5个用户数据），写放大是 $9/1.5=6$ 。

如果整个SSD闪存空间不变，还是216个小方块，调整OP比例至72个小方块（牺牲用户空间，OP比例50%），因此，SSD容量就变成144个小方块。144个小方块的用户数据平均分摊到216个小方块时，每个小方块的平均有效数据为 $144/216=0.67$ ，一个闪存块上的有效数据为 $0.67 \times 9 \approx 6$ ，也就是一个闪存块上面平均有6个浅色块和3个深色块。为了写3个用户数据方块，需要写9个方块的数据（原有6个有效数据，加3个用户数据），写放大是 $9/3=3$ 。

从上可见，OP越大，写放大越小。很好理解，OP越大，每个闪存块有效数据越少，垃圾越多，因此需要重写更少的数据，因此写放大越小。同时，由于GC需要重写的垃圾数据越少，SSD满盘写性能也越好。

当然，上面说的都是最坏的情况（垃圾数据平均分摊到每个闪存块上）。现实是，垃圾数据大多数时候并不是平均分配到每个闪存块上，有些块上的垃圾多，有些块上的垃圾少，实际GC挑选闪存块，是挑垃圾多的，因此，实际写放大是小于前面的计算值的。

OP大小和写放大以及SSD耐写度的关系如图4-25所示。

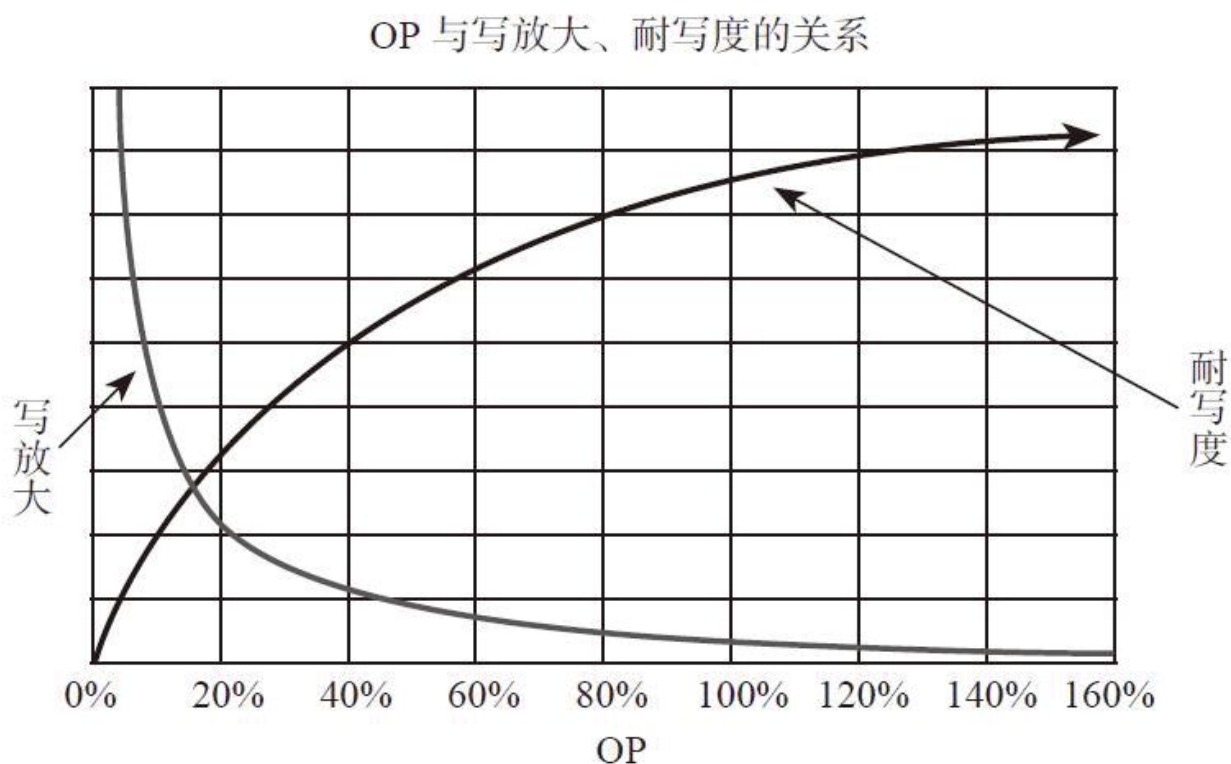


图4-25 OP大小对写放大和耐写度的影响

总结一下：WA越小越好，因为越小意味着对闪存的损耗越小，可以延长闪存使用寿命，从而支持更多的用户数据写入量；OP越大越好，OP越大，意味着写放大越小，也意味着SSD写性能越好。

影响写放大的因素主要有：

- OP：OP越大，WA越小。

·用户写入的数据**Pattern**：如前文所见，如果数据都是顺序写入，GC做的量就少（最好的情况是整个闪存块都是无效数据，只需擦除，无需数据搬移），写放大小。

·GC策略：在挑选源闪存块的时候，如果不挑选有效数据最少（垃圾数据最多）的块作为源闪存块，就会增加写放大；另外，控制后台GC产生空闲闪存块的数量，也能减小写放大。

·磨损平衡：为平衡每个闪存块的擦除次数，需要数据的搬移。

·读干扰（**Read disturb**）和数据保存处理（**Data Retention handling**）：数据搬移增加写放大。

·主控：带压缩和不带压缩的控制器肯定会影响写放大。

·Trim：有没有Trim，对写放大影响很大。

4.3.3 垃圾回收实现

垃圾回收可以简单地分为三步：

- 1) 挑选源闪存块。
- 2) 从源闪存块中找有效数据。
- 3) 把有效数据写入到目标闪存块。

挑选源闪存块，一个常见的算法就是挑选有效数据最小的块，这样需要重写的有效数据就越少，写放大自然最小，回收一个块付出的代价也最小。那么，Die中那么多闪存块，怎么就能一下子找到有效数据最小的那个块呢？

这需要固件在写用户数据时做一些额外的工作，即记录和维护每个用户闪存块的有效数据量。用户每往一个新的块上写入一笔用户数据，该闪存块上的有效数据数就加1。同时还需要找到这笔数据之前所在的块（如果之前该笔数据曾写入过），由于该笔数据写入到新的块，那么在原闪存块上的数据就变无效了，因此原闪存块上的有效数据量应该减1。

还是以前面的小型SSD为例：

当用户没有写入任何数据时，所有闪存块上的有效数据都为0，如表4-3所示。

表4-3 初始化每个闪存块的有效数据

闪存块号	有效数据量	闪存块号	有效数据量
0	0	3	0
1	0	4	0
2	0	5	0

当往Block 0上写入逻辑页1、2、3、4后，Block 0的有效数据就变成4（见图4-26和表4-4）。

当用户空间写满后，每个闪存块上有效数据如图4-27和表4-5下所示。

覆盖写后，用户空间如图4-25所示。

由于逻辑页1、2、3、4写入到Block 5上，Block 5上的有效数据变成4，所以逻辑页1、2、3、4在之前所在的Block 0上变成无效，因此在写入逻辑页1、2、3、4的时候，不仅要更新Block 5上的有效数据为4，还应该把Block 0上的有效数据相应地减少4，如表4-6所示。

	CH0			CH1			CH2			CH3		
Block 0	1			2			3			4		
Block 1												
Block 2												
Block 3												
Block 4												
Block 5												

图4-26 Block 0上写入4个逻辑页
表4-4 Block 0有效数据更新为4

闪存块号		有效数据量		闪存块号		有效数据量	
0		4		3		0	
1		0		4		0	
2		0		5		0	

	CH0			CH1			CH2			CH3		
	1	5	9	2	6	10	3	7	11	4	8	12
Block 0	13	17	21	14	18	22	15	19	23	16	20	24
	25	29	33	26	30	34	27	31	35	28	32	36
	37	41	45	38	42	46	39	43	47	40	44	48
Block 1	49	53	57	50	54	58	51	55	59	52	56	60
	61	65	69	62	66	70	63	67	71	64	68	72
	73	77	81	74	78	82	75	79	83	76	80	84
Block 2	85	89	93	86	90	94	87	91	95	88	92	96
	97	101	105	98	102	106	99	103	107	100	104	108
	109	113	117	110	114	118	111	115	119	112	116	120
Block 3	121	125	129	122	126	130	123	127	131	124	128	132
	133	137	141	134	138	142	135	139	143	136	140	144
	145	149	153	146	150	154	147	151	155	148	152	156
Block 4	157	161	165	158	162	166	159	163	167	160	164	168
	169	173	177	170	174	178	171	175	179	172	176	180
Block 5												

图4-27 首次写满用户空间
表4-5 首次用户空间写满后闪存块上有效数据统计

闪存块号	有效数据量	闪存块号	有效数据量
0	36	3	36
1	36	4	36
2	36	5	0

	CH0			CH1			CH2			CH3		
	1	5	9	2	6	10	3	7	11	4	8	12
Block 0	13	17	21	14	18	22	15	19	23	16	20	24
	25	29	33	26	30	34	27	31	35	28	32	36
	37	41	45	38	42	46	39	43	47	40	44	48
Block 1	49	53	57	50	54	58	51	55	59	52	56	60
	61	65	69	62	66	70	63	67	71	64	68	72
	73	77	81	74	78	82	75	79	83	76	80	84
Block 2	85	89	93	86	90	94	87	91	95	88	92	96
	97	101	105	98	102	106	99	103	107	100	104	108
	109	113	117	110	114	118	111	115	119	112	116	120
Block 3	121	125	129	122	126	130	123	127	131	124	128	132
	133	137	141	134	138	142	135	139	143	136	140	144
	145	149	153	146	150	154	147	151	155	148	152	156
Block 4	157	161	165	158	162	166	159	163	167	160	164	168
	169	173	177	170	174	178	171	175	179	172	176	180
	1			2			3			4		
Block 5												

图4-28 用户空间写满后继续写入4个逻辑页
表4-6 覆盖写后SSD中闪存块有效数据统计

闪存块号	有效数据量	闪存块号	有效数据量
0	32	3	36
1	36	4	36
2	36	5	4

由于固件维护了每个闪存块的有效数据量，因此在GC的时候能快速找到有效数据最少的那个块。

挑选有效数据最少的那个块作为源闪存块，这种BPA算法叫作Greedy算法，是绝大多数SSD采用的一种策略。除此之外，还有其他的BPA算法。比如，除了基于闪存块有效数据量，有些SSD在挑选源闪存块时，还把闪存块的擦写次数考虑进去了，这其实暗藏着磨损平衡算法（后面会详细介绍）。挑选闪存块时，一方面，我们希望挑有效数

据最少的（快速得到一个新的闪存块）；另一方面，我们期望挑选擦写次数最小的（分摊擦写次数到每个闪存块）。如果两者都具备，那最好不过了。但现实是，擦写次数最小的闪存块，有效数据未必最少；有效数据最少的闪存块，擦写次数未必最小。因此，需要给有效数据和擦写次数设定一个权重因子，进而得到一个最优的选择。这种方法的好处是可以把磨损平衡算法做到GC中来，可以不需要额外的磨损平衡算法；缺点是相对单纯只看有效数据策略的GC，由于挑选的闪存块可能有效数据很多，因此写放大变大，GC性能变差。

其实还有很多BPA算法（可以上www.ssfans.com 查看相关文章），但在实际的SSD产品中，主要还是应用前面提到的两种策略，简单实用。

这是GC的第一步，挑选源闪存块。

第二步就是把数据从源闪存块读出来。这里也是有讲究的，怎么读才是最有效率的？全部读出来还是只读有效数据？有人说，当然只读有效数据更有效率了，毕竟我们只需重写有效数据。我赞同这个观点，但问题来了，一个闪存块有那么多逻辑页数据，如何知道哪些数据是有效，哪些又是无效的呢？如图4-29所示。

	CH0			CH1			CH2			CH3		
Block 0	154	108	121	46	11	110	37	110	157	134	73	31
	123	19	131	6	45	173	54	35	71	165	96	141
	164	134	57	109	172	86	158	59	107	109	118	34
Block 1	10	54	135	68	90	10	150	100	22	167	126	119
	104	98	63	85	46	94	148	123	7	17	176	59
	27	22	118	50	51	28	91	40	110	3	161	103
Block 2	57	3	115	21	114	144	157	98	54	132	71	24
	76	48	83	111	106	120	54	34	179	152	47	106
	26	1	106	179	137	112	6	38	107	20	167	49
Block 3	17	84	177	155	3	149	172	160	80	52	20	57
	45	78	141	141	70	37	178	66	56	61	119	163
	106	135	43	55	93	166	172	103	44	164	119	150
Block 4	172	132	3	150	79	173	148	172	11	133	175	68
	34	118	169	34	2	162	16	156	66	30	79	117
	8	12	90	92	22	88	153	81	83	53	13	26
Block 5	20	157	106	180	155	131	82	53	59	72	26	1
	14	132	20	151	82	128	77	168	9	113	111	22
	96	175	111	83	28	60	178	126	22	166	135	9

图4-29 用户数据随机分布在SSD内

当我们挑选Block 0（有效数据最少）来做垃圾回收时，如果只读出有效数据（浅色方块），FW如何知道Block 0上哪些数据是有效的呢？办法总是有的。

前面提到，固件在往一个闪存块上写入逻辑页时，会更新和维护闪存块的有效数据量，因此可以快速挑中源闪存块。更进一步，如果固件不仅仅只更新和维护闪存块的有效数据量，还给闪存块一个Bitmap表，标识哪个物理页（例子中我们假设逻辑页和闪存页大小一样）是否有效，那么在做GC的时候，固件只需根据Bitmap表的信息，把有效数据读出，然后重写即可。具体做法跟前面介绍的类似，即固件把一笔逻辑页写入到某个闪存块时，该闪存块上对应位置的Bit就置成1。一个闪存块上新增一笔有效数据，就意味着该笔数据所在的前一

个闪存块上数据变成无效，因此需要把前一个闪存块对应的位置的Bit清0（见图4-30）。

		CH0			CH1			CH2			CH3		
		1			2			3			4		
Block 0													
Block 1													
Block 2													
Block 3													
Block 4													
Block 5													

图4-30 SSD首次写入4个逻辑页数据

固件往Block 0写入逻辑页0、1、2、3后，Bitmap信息如表4-7所示。

表4-7 向Block 0写入后SSD中有效数据Bitmap

闪存块号	有效数据量	有效数据 Bitmap(块内第一行)	闪存块号	有效数据量	有效数据 Bitmap(块内第一行)
0	4	100 100 100 100	3	0	000 000 000 000
1	0	000 000 000 000	4	0	000 000 000 000
2	0	000 000 000 000	5	0	000 000 000 000

固件写满后，整个用户空间如图4-31所示。

覆盖写后，用户空间如图4-32所示。

在写入逻辑页1、2、3、4的时候，不仅要更新Block 5上的Bitmap，还应该把Block 0（逻辑页1、2、3、4之前所在的闪存块）上对应的Bits清0，如表4-9所示。

由于有了闪存块上有效数据的Bitmap，在GC读的时候，固件就能准确定位到有效数据并读出。Bitmap存在的好处，就是使GC更有效率，但固件需要付出额外的代价去维护每个闪存块的Bitmap。在我们的例子中，每个闪存块（这里指的是所有Die上同一个闪存块号组成的闪存块集合）只有36个逻辑页，但在实际情况下，每个闪存块有可能存在一两千个闪存页，每个闪存页可以容纳若干个逻辑页，因此，每个闪存块的Bitmap需要占用数目不小的存储空间。对带DRAM的SSD来说，Bitmap的存储空间可能不是问题，但对没有DRAM的SSD来说，可能就没有那么多的SRAM来存储所有闪存块的Bitmap。对DRAM-Less的SSD来说，由于SRAM受限，只能在SRAM中加载部分闪存块的Bitmap，因此还需要Bitmap的换入换出（同Map Table），给固件带来不小的开销，实现起来没有想象中的简单。

		CH0				CH1				CH2				CH3			
Block 0		1	5	9	2	6	10	3	7	11	4	8	12				
		13	17	21	14	18	22	15	19	23	16	20	24				
		25	29	33	26	30	34	27	31	35	28	32	36				
Block 1		37	41	45	38	42	46	39	43	47	40	44	48				
		49	53	57	50	54	58	51	55	59	52	56	60				
		61	65	69	62	66	70	63	67	71	64	68	72				
Block 2		73	77	81	74	78	82	75	79	83	76	80	84				
		85	89	93	86	90	94	87	91	95	88	92	96				
		97	101	105	98	102	106	99	103	107	100	104	108				
Block 3		109	113	117	110	114	118	111	115	119	112	116	120				
		121	125	129	122	126	130	123	127	131	124	128	132				
		133	137	141	134	138	142	135	139	143	136	140	144				
Block 4		145	149	153	146	150	154	147	151	155	148	152	156				
		157	161	165	158	162	166	159	163	167	160	164	168				
		169	173	177	170	174	178	171	175	179	172	176	180				
Block 5																	

图4-31 首次SSD用户空间写满后
表4-8 用户空间写满后各个闪存块的Bitmap

闪存块号	有效数据量	有效数据 Bitmap(块内第一行)	闪存块号	有效数据量	有效数据 Bitmap(块内第一行)
0	36	111 111 111 111	3	36	111 111 111 111
1	36	111 111 111 111	4	36	111 111 111 111
2	36	111 111 111 111	5	0	000 000 000 000

		CH0				CH1				CH2				CH3			
		1	5	9		2	6	10		3	7	11		4	8	12	
Block 0		13	17	21		14	18	22		15	19	23		16	20	24	
		25	29	33		26	30	34		27	31	35		28	32	36	
		37	41	45		38	42	46		39	43	47		40	44	48	
Block 1		49	53	57		50	54	58		51	55	59		52	56	60	
		61	65	69		62	66	70		63	67	71		64	68	72	
		73	77	81		74	78	82		75	79	83		76	80	84	
Block 2		85	89	93		86	90	94		87	91	95		88	92	96	
		97	101	105		98	102	106		99	103	107		100	104	108	
		109	113	117		110	114	118		111	115	119		112	116	120	
Block 3		121	125	129		122	126	130		123	127	131		124	128	132	
		133	137	141		134	138	142		135	139	143		136	140	144	
		145	149	153		146	150	154		147	151	155		148	152	156	
Block 4		157	161	165		158	162	166		159	163	167		160	164	168	
		169	173	177		170	174	178		171	175	179		172	176	180	
		1				2				3				4			
Block 5																	

图4-32 用户空间写满后继续写入4个逻辑页

表4-9 覆盖写后各个闪存块的Bitmap

闪存块号	有效数据量	有效数据 Bitmap(块内第一行)	闪存块号	有效数据量	有效数据 Bitmap(块内第一行)
0	36	<u>0</u> 11 <u>0</u> 11 <u>0</u> 11 <u>0</u> 11	3	36	111 111 111 111
1	36	111 111 111 111	4	36	111 111 111 111
2	36	111 111 111 111	5	0	<u>1</u> 00 <u>1</u> 00 <u>1</u> 00 <u>1</u> 00

如果没有每个闪存块的有效数据Bitmap，FW做GC的时候，可以选择把所有数据读上来。但此时还需要解决一个问题，那就是这些数据哪些是有效的呢？也就是哪些数据需要重写呢？

SSD在把用户数据写到闪存的时候，会额外打包一些数据，我们叫它元数据（Meta Data），它记录着该笔用户数据的相关信息，比如该

笔数据对应的逻辑地址、数据长度，以及时间戳（数据写入到闪存的时间）等。因此，用户数据在闪存中是像图4-33这样存储的。

	元数据	用户数据
Pa 1	La 1, TS1..	User data 1
Pa 2	La 2, TS2..	User data 2
Pa 3	La 3, TS3..	User data 3
Pa 4	La 4, TS4..	User data 4
Pa 5	La 5, TS5..	User data 5
Pa 6	La 6, TS6..	User data 6
Pa 7	La 7, TS7..	User data 7
Pa 8	La 8, TS8..	User data 8
Pa 9	La 9, TS9..	User data 9
...
Pa x-1	La x-1, TS..	User data x-1
Pa x	La x, TS..	User data x

Pa: Physical Address，物理地址
La: Logical Address，逻辑地址
TS: Timestamp，时间戳

图4-33 元数据和用户数据存储的例子

GC的时候，FW把数据读上来，就获得了该笔数据对应的LBA，要判断该数据是否无效，需要查找映射表，获得该LBA对应的物理地址，如果该地址与该数据在闪存块上的地址一致，就说明是有效的，否则该数据就是无效的。

把源闪存块里的全部数据读出来，这种方式的缺点显而易见：GC做得慢。不管数据是否有效（读之前不知道是否有效），都需要读出来，然后还需要查找映射表来决定该笔数据是否无效。这对带DRAM的SSD来说问题不大，因为其所有映射表都在DRAM中，但对DRAM-Less的SSD来说，很多时候都需要从闪存里面把映射关系读上来，这简直是个灾难。这种方式的好处就是FW实现起来简单，不需要维护额外类似闪存块有效数据Bitmap之类的东西，不需要额外的RAM资源和FW开销。

还有一个折中的办法。就是除了维护L2P（Logical to Physical）的映射表，还维护一张P2L（Physical to Logical）的表。该表记录了每个闪存块写入的LBA，该P2L数据写在该闪存块的某个位置（或单独存储）。当回收该闪存块时，首先把该P2L表加载上来，然后根据上面的LBA，依次查找映射表，决定该数据是否有效，有效的数据会被读出来，然后重新写入。采用该方法，不需要把该闪存块上的所有数据一股脑地读出来，但还是需要查找映射表以决定数据是否有效。因此，该方法在性能上介于前面两种方法之间，在资源和固件开销上也是处于中间的。

当有效数据读出来时，最后一步就是重写，即把读出来的有效数据写入闪存。

4.3.4 垃圾回收时机

SSD什么时候做GC？当用户写入数据时，如果可用的闪存块小于一定阈值，这时就需要做GC，以腾出空间给用户写。这时做的GC，叫作**Foreground GC**（前台垃圾回收）。这是被动方式，它是由于SSD没有多少可用的闪存块时，才去做的GC。与之相对应的，就是**Background GC**（后台垃圾回收），它是在SSD空闲（Idle）的时候，SSD主动去做的GC，这样在用户写入的时候就有充裕的可用闪存块，不需要临时抱佛脚（做**Foreground GC**），从而改善用户写入性能。但是，出于功耗考虑，有些SSD可能就不做后台垃圾回收了，当SSD空闲后，直接进入省电模式，或者做少量的GC，然后进入省电模式。

这是常见的两种垃圾回收时机，都是SSD自己内部控制的。事实上，除了SSD本身，有些SSD还支持主机控制其去做GC。这个比较有意思，我们花点时间来看看。

2015年8月15日，OCZ发布了一款SATA接口企业级SSD——**Saber 1000HMS**，它是首款具有“主机管理SSD”（**Host Managed SSD**，**HMS**）功能的SSD。所谓**HMS**，就是主机通过应用软件获取SSD的运行状态，然后控制SSD的一些行为。

在SSD的内部，运行着一些后台任务，比如垃圾回收、记录SSD运行日志等。这些后台任务的执行，会影响SSD的性能，并且使得SSD的时延（**latency**）不可预测。**HMS**技术使得主机能控制SSD的后台任务，后台任务执行或者不执行，什么时候执行，什么时候不执行，主机是可控的。

这有什么用呢？对单个SSD来说，使用者可以通过**HMS**软件，在SSD空闲时让其执行垃圾回收任务，这样，在后续的写入过程中，SSD内部有足够的空闲块可写，不需要临时去做垃圾回收，从而提升SSD性能，减小写入的时延。

Saber 1000HMS是企业级的SSD。相比客户级SSD，稳定的性能和时延是企业级更加追求的。后台任务的存在，使得SSD性能和时延很难保持一致。**HMS**技术的出现，使得整个系统具有稳定的性能和可预测的时延，如图4-34所示。

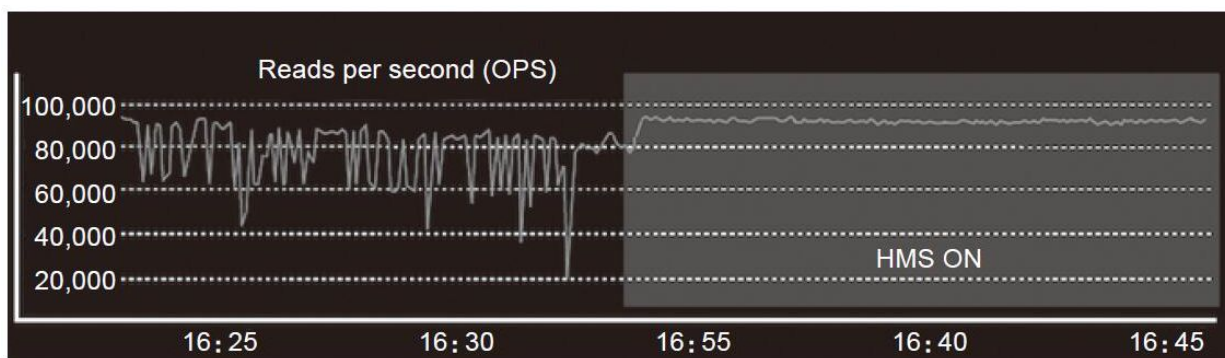


图4-34 HMS打开后系统性能平稳

4.4 Trim

对于一个文件**File A**来说，用户看到的是文件，操作系统把文件划分为若干个逻辑块，然后写入**SSD**的闪存空间。当用户删除掉文件**File A**时，其实它只是切断用户与操作系统的联系，即用户访问不到这些地址空间；而在**SSD**内部，逻辑页与物理页的映射关系还在，文件数据在闪存当中也是有效的，如图4-35所示。

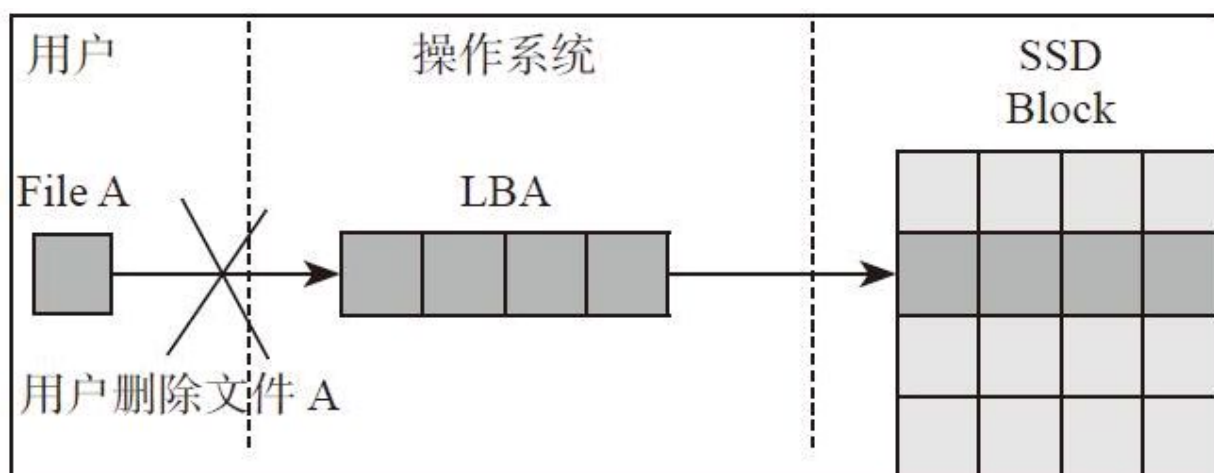


图4-35 用户删除文件示例

在没有**Trim**之前，**SSD**无法知道那些被删除的数据页是否无效，必须等到系统要求在相同的地方（用户空间、逻辑空间）写入数据时才知道那些数据是无效的，进而放心删除。由于**SSD**不知道这些删除的数据已经无效，在做垃圾回收的时候，仍把它当作有效数据进行数据的搬移，这不仅影响到**GC**的性能，还影响到**SSD**的寿命（写放大增大）。

Trim是一个新增的**ATA**命令（**Data Set Management**），专为**SSD**而生。当用户删除一个文件时，操作系统（对**Windows**来说，它自**Windows 7**开始支持**Trim**）会发**Trim**命令给**SSD**，告诉**SSD**该文件对应的数据无效了。一旦**SSD**知道哪些数据无效之后，在做垃圾回收的时候就可以把这些删除掉的数据抛弃掉，不做无谓的数据搬移。这样不仅增强了**SSD**的性能，还延长了**SSD**寿命。

SCSI里面的同等命令叫UNMAP，NVMe里面叫Deallocate。它们指的都是同一个功能。

当SSD收到Trim命令时，它要做些什么呢？

举个例子。主机通过Trim命令告诉SSD：我0~7的逻辑页上的数据删除了，你可以把它们当垃圾处理。收到Trim命令之前，逻辑页0~7有以下映射，它们分别写在物理地址PBA a~h，如图4-36所示。

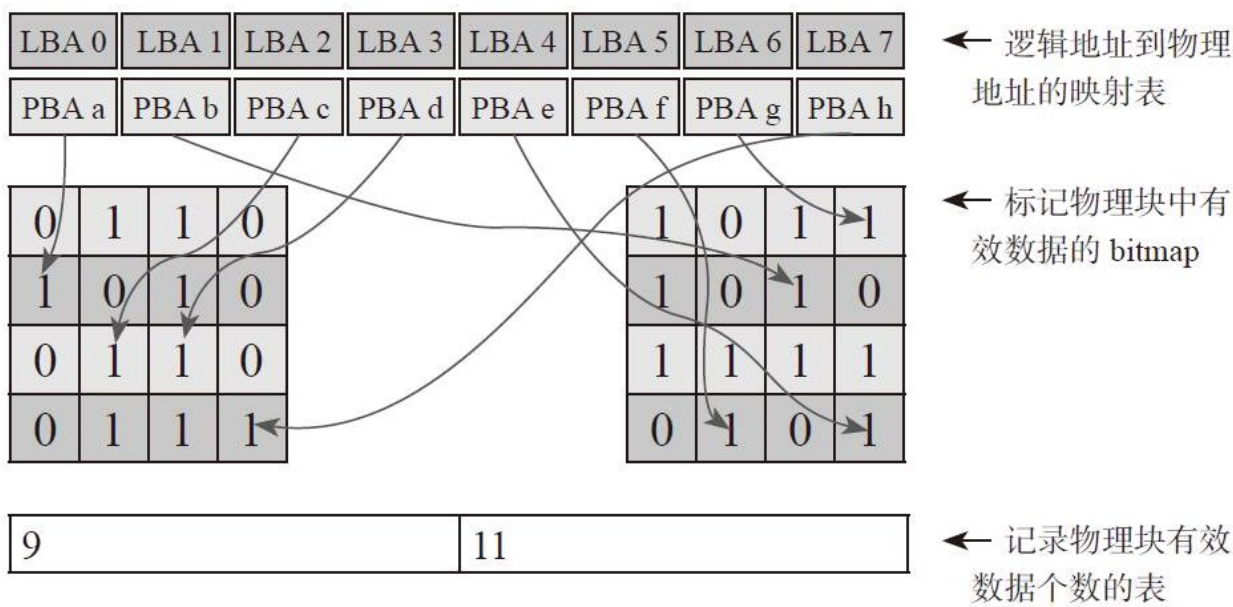


图4-36 FTL中的3张表

如前所述，一般FTL都有这3个表。FTL映射表记录每个LBA对应的物理页位置。Valid Page Bit Map (VPBM) 记录每个物理块上哪个页有有效数据，Valid Page Count (VPC) 则记录每个物理块上的有效页个数。通常GC会使用VPC进行排序来回收最少有效页的闪存块；VPBM则是为了在GC时只读有用的数据，也有部分FTL会省略这个表。

如图4-36所示，FTL的映射往往是非常分散的，连续的逻辑页对应地址会在很多不同的闪存块上。SSD收到Trim命令后，为了实现数据删除，固件要按顺序做以下的事情（图4-37中的步骤1~4）。



图4-37 FTL处理TRIM流程

Trim的实现逻辑基本就是这样，不同的SSD实现可能略有不同，比如如果没有有效数据Bitmap，就没有图4-37中的第2步操作。需要说明的是，图4-37中的步骤5~7是Trim命令处理后，GC的处理，它们不是Trim命令处理的部分。Trim命令是不会触发GC的。

关于Trim的更多内容，可以上www.ssdfans.com 搜索Trim相关的文章。

4.5 磨损平衡

磨损平衡，就是让SSD中的每个闪存块的磨损（擦除）都保持均衡。

为什么要做磨损平衡？原因是闪存都是有寿命的，即闪存块有擦写次数限制。一个闪存块，如果其擦写次数超过一定的值，那么该块就变得不那么可靠了，甚至变成坏块不能用了。如果不做磨损平衡，则有可能出现有些闪存块频繁拿来擦写，这些闪存块很容易就会寿终正寝。随着不断的写入，越来越多的坏块出现，最后导致SSD在保质期前就挂掉。相反，如果让所有闪存块一起来承担，则能经受更多的用户数据写入。

一个闪存块寿命有多长呢？从SLC十几万的擦写次数，到MLC几千的擦写次数，然后到TLC的一两千次甚至几百次擦写次数，随着闪存工艺不断向前推，闪存的寿命越来越短，SSD对磨损平衡的处理要求也越来越高，如图4-38所示。

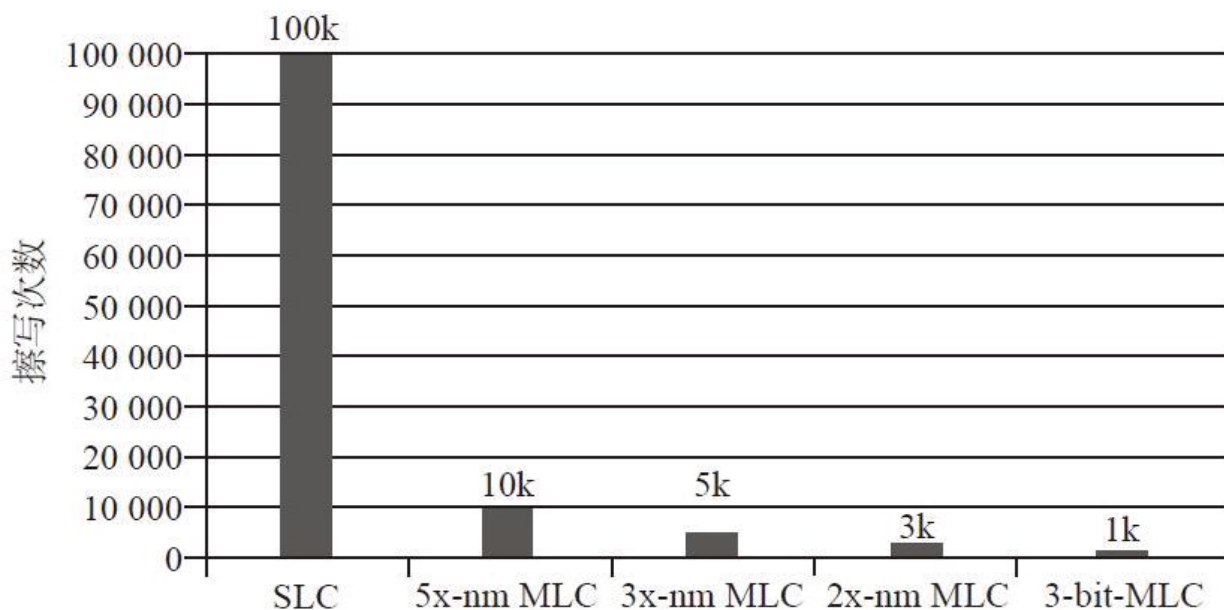


图4-38 不同制程和类型闪存的擦写次数

接下来的问题就是，SSD是怎么做磨损平衡的呢？

在这之前，我们先抛出几个概念：冷数据（Cold Data）和热数据（Hot Data），年老的（Old）块和年轻的（Young）块。

所谓冷数据，就是用户不经常更新的数据，比如用户写入SSD的操作系统数据、只读文件数据、小电影等；相反，热数据就是用户更新频繁的数据。数据的频繁更新，会在SSD内部产生很多垃圾数据（新的数据写入导致老数据失效）。

所谓年老的块，就是擦写次数比较多的闪存块；擦写次数比较少的闪存块，年纪相对小，我们叫它年轻的块。SSD很容易区分年老的块和年轻的块，看它们的EC（Erase Count，擦除次数）就可以了，大的就是老的，小的就是年轻的。

SSD一般有动态磨损平衡（Dynamic WL）和静态磨损平衡（Static WL）两种算法。动态磨损平衡算法的基本思想是把热数据写到年轻的块上，即在拿一个新的闪存块用来写的时候，挑选擦写次数小的；静态磨损平衡算法基本思想是把冷数据写到年老的块上，即把冷数据搬到擦写次数比较多的闪存块上。

动态磨损平衡可能相对好理解一些：在写入新数据时，挑选年轻力壮的闪存块，这样就避免了一直往年长的闪存块上写入数据，闪存块的擦写次数能保持一个比较均衡的值。

我们重点来说说静态磨损平衡。

为什么还需要静态磨损平衡？冷数据由于不经常更新，它写在一个或者几个闪存块上后，基本保持不动，这样，这些闪存块的擦写次数就不会增加；相反，对别的闪存块，由于经常拿来写入用户数据，擦写次数是一直增长的。这样就导致闪存块的擦写不均衡，这不是我们期望的。因此，固件需要做静态磨损平衡，把冷数据搬到擦写次数比较多的闪存块上，让那些劳苦功高的年老闪存块休息一下，腾出来的年轻闪存块去替年老的闪存块承受用户数据的写入。

固件具体做静态磨损平衡的时候，一般使用GC机制来做，只不过它挑选源闪存块时，不是挑选有效数据最小的闪存块，而是挑选冷数据所在的闪存块。其他和GC差不多，即读取源闪存块上的有效数据，然后把它写到擦写次数相对大的闪存块上去。

静态磨损平衡可能导致冷数据和热数据混在同一个闪存块上，即冷数据可能跟用户刚写入的数据混在一起，或者冷数据和GC的数据写在一起，或者三者写在一起。

1) SWL数据和用户数据混在一起写在同一个闪存块上，如图4-39所示。

2) SWL数据和GC数据混在一起写在同一个闪存块上，如图4-40所示。



图4-39 SWL和用户数据写在一起



图4-40 SWL和GC数据写在一起

3) 三者全都混在一起写在同一个闪存块上，如图4-41所示。

为什么我要提冷热数据混在一起写这个问题？冷热数据混在一起写不好吗？

的确有不好的地方，那就是在做GC的时候，由于冷数据掺杂其中（冷数据由于不经常被用户更改，这些数据往往是有效数据），这些冷数据就可能经常地从一个闪存块搬到另外一个闪存块，然后从另外一个闪存块再搬到别的闪存块上去，长此以往，引入了不少额外的写，导致写放大增大。

有读者要问，那该怎么办？下面提供一种解决方案。

解决办法如图4-42所示，做静态磨损平衡的时候，用专门的闪存块来放冷数据，即不与用户或者GC写入同一个闪存块。这样冷数据就单独写在某些闪存块上，它们一般不会挑选为GC的源闪存块，也就避免了这些冷数据的频繁搬移。它只有在下一次需要做静态磨损平衡的时候，才会从一个闪存块搬到另外一个闪存块。

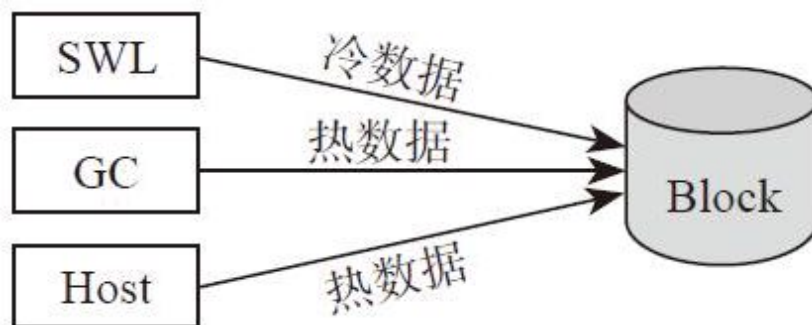


图4-41 SWL，GC和用户数据混在一起写

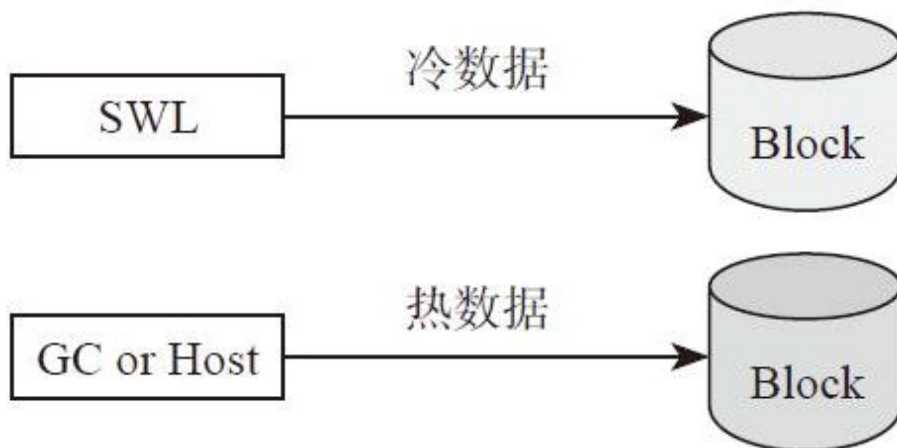


图4-42 冷热数据分开存储

不同的SSD有不同的静态磨损平衡做法。如果不在乎写放大（EC预算够大，不差钱），也不在乎冷数据搬移导致的性能下降，那么冷热数据混在一起就一起，毕竟实现简单（不需要另外管理静态磨损平衡的闪存块）；相反，如果对写放大比较敏感的话，那么最好还是冷热数据分开。

4.6 掉电恢复

掉电分两种，一种是正常掉电，另一种是异常掉电。不管是哪种原因导致的掉电，重新上电后，SSD都需要能从掉电中恢复过来，继续正常工作。

先说正常掉电。在掉电前，主机会通过命令通知SSD，比如SATA中的Idle Immediately，SSD收到该命令后，主要会做以下事情：

- 把buffer中缓存的用户数据刷入闪存。

- 把映射表刷入闪存。

- 把闪存的块信息写入闪存（比如当前写的是哪个闪存块，以及写到该闪存块的哪个位置，哪些闪存块已经写过，哪些闪存块又是无效的等）。

- 把SSD其他信息写入闪存。

主机等SSD处理完以上事情后，才会真正停止对SSD的供电。正常掉电不会导致数据的丢失，重新上电后，SSD只需把掉电前保存的相关信息（比如映射数据，闪存块信息等）重新加载，又能接着掉电前的状态继续工作。

如果SSD世界只存在正常掉电，那么SSD的实现就会简单很多。可是，突如其来的掉电（异常掉电），对SSD来说，没有“喜”，只有“惊”。

所谓的异常掉电，就是SSD在没有收到主机的掉电通知时就被断电；或者收到主机的掉电通知，但还没有来得及处理上面提到的那些事情，就被断电了。异常掉电可能会导致数据的丢失，比如缓存在SSD中的数据来不及写到闪存，掉电导致这部分数据丢失。还有，根据闪存特性，如果掉电发生在写MLC的Upper page，会导致其对应的Lower Page数据遭到破坏，也就是意味着之前写入闪存的数据也可能由于异常掉电导致丢失。异常掉电恢复的目的一方面是尽可能恢复用户数据，把损失减到最低；另一方面是让SSD经历异常掉电后还能正常工作。

本节主要介绍异常掉电处理。

SSD为什么怕异常掉电？它不是用闪存做存储介质吗？它不是数据掉电不丢失吗？没错。不过一个**SSD**，除了数据掉电不丢失的闪存，还需要有掉电数据丢失的**RAM**、**SRAM**或者**DRAM**。闪存的作用是存储数据，而**RAM**的作用主要是**SSD**工作时用以缓存用户数据和存放映射表（**Map Table**，逻辑地址映射闪存物理地址）。所以一旦掉电，**RAM**的数据就会丢失。

为防止异常掉电导致的数据丢失，一个简单的设计就是在**SSD**上加电容，**SSD**一旦检测到掉电，就让电容开始放电，然后把**RAM**中的数据刷到闪存上面去，从而避免数据丢失。企业级的**SSD**一般都带有电容。带电容的**SSD**，还是需要设计异常掉电处理模块，因为电容不能100%保证**SSD**在掉电前把所有的信息刷入闪存。

还有一个比较前卫的想法，就是把**RAM**这种Volatile（掉电数据丢失）的东西，用Non-Volatile（掉电数据不丢失）的东西来替代，但要求这种Non-Volatile的东西性能上接近**RAM**。这样，整个**SSD**都是Non-Volatile的了。Intel和Micron合作开发的3D XPoint，可作为一个选择。3D XPoint兼有闪存掉电数据不丢失和内存快速访问的特点。

RAM中缓存的用户数据，主机自认为把它们写到**SSD**了（非FUA命令，数据写到缓存，**SSD**就返回状态给主机），但**SSD**只是把它们缓存在**RAM**中，并没有写到闪存。异常掉电时，如果**SSD**上没有使用电容，也没有使用其他黑科技，这部分数据便损失无疑。重上电时，主机是再也读不到这些数据了。

掉电还会导致**RAM**中映射表丢失。映射表数据很重要，对一个逻辑地址，如果**SSD**查找不到对应的物理地址，它就无法从闪存上读取数据返回给主机。如果映射表中的数据不是最新的，旧的物理地址对应着老的数据，**SSD**就会错误地把老数据返回给主机，这个问题就严重了。

阿呆原账户上有10元钱，最近存入100万元，但由于异常掉电导致银行没有把100万元写入数据库，下次阿呆到ATM上一看，怎么还是10元钱？阿呆当时就昏死过去！异常掉电害死人。

但是，和RAM中用户数据丢失不同，RAM中映射表数据是有办法恢复过来的。SSD的异常掉电恢复主要就是映射表的恢复重建。

那么，如何重建映射表呢？下面介绍一种重构策略（不同的SSD重构策略略有不同，但大同小异）。SSD在把用户数据写到闪存的时候，会额外打包一些数据，我们叫它元数据（Meta Data），它记录着该笔用户数据的相关信息，比如该笔数据对应的逻辑地址、数据写入时间（时间戳）等，如图4-43所示。

元数据：

逻辑地址（LBA）	时间戳（TS）	其他内容
-----------	---------	------

图4-43 元数据内容示例

因此，用户数据在闪存中是像下面这样存储的（见图4-44）。

闪存空间		
	元数据	用户数据
Pa 1	La 1, TS1..	User data 1
Pa 2	La 2, TS2..	User data 2
Pa 3	La 3, TS3..	User data 3
Pa 4	La 4, TS4..	User data 4
Pa 5	La 5, TS5..	User data 5
Pa 6	La 6, TS6..	User data 6
Pa 7	La 7, TS7..	User data 7
Pa 8	La 8, TS8..	User data 8
Pa 9	La 9, TS9..	User data 9
...
Pa x-1	La x-1, TS..	User data x-1
Pa x	La x, TS..	User data x

Pa: Physical Address, 物理地址

La: Logical Address, 逻辑地址

TS: Timestamp, 时间戳

图4-44 元数据和用户数据存储示例

以图4-44为例，如果我们读取物理地址Pa x，就能读取到元数据x和用户数据x，而元数据是有逻辑地址La x的，因此，我们就能获得映射：La x→Pa x。映射表的恢复原理其实很简单，只要全盘扫描整个闪存空间，就能获得所有的映射关系，最终完成整个映射表的重构。

原理简单，但实现起来还有一些问题需要考虑，比如如何解决数据新旧问题、重构速度问题等。

同一逻辑地址，用户可能写过若干次，在闪存空间，该逻辑地址对应的数据有很多是旧数据，只有一笔是新数据，那么如何甄别哪些数据是旧的，哪些数据是新的呢？如何让逻辑地址映射到最新数据所在的物理地址呢？以图4-44为例，SSD起初把逻辑地址La 2的数据写在物理地址Pa 2上；之后，用户又改写了那笔数据，SSD把它写到了物理地址Pa 8上。我们知道，用户最后写入的数据总是最新的。在这里，时间戳帮上大忙了，哪个值大，就表示哪个是最后写入的。SSD可以依赖Meta data中的时间戳来区分新旧数据的。图4-44中，在全盘扫描时，假设扫描顺序是从物理地址Pa 1到物理地址Pa x，对逻辑地址La 2来说，开始会产生映射La 2 → Pa 2，但扫描到Pa 8时，发现时间戳比之前的更新，于是新的映射取代旧的映射，最后得到映射关系：La 2 → Pa 8。

全盘扫描有一个问题，就是映射表恢复很慢，所耗的时间与SSD容量成正比。现在SSD容量已达到TB级别，全盘扫描映射方式，重构映射表需要花费几分钟甚至几十分钟，这在实际使用中，用户是不能接受的。那SSD内部是如何快速恢复映射表的呢？

一种办法就是SSD定期把SSD中RAM的数据（包括映射表和缓存的用户数据）和SSD相关的状态信息（诸如闪存块擦写次数、闪存块读取次数、闪存块其他信息等）写入到闪存中去，与正常掉电前SSD要做的事情类似，这个操作我们称之为做Checkpoint（检查点，此处译成“快照”更合适），如图4-45所示。

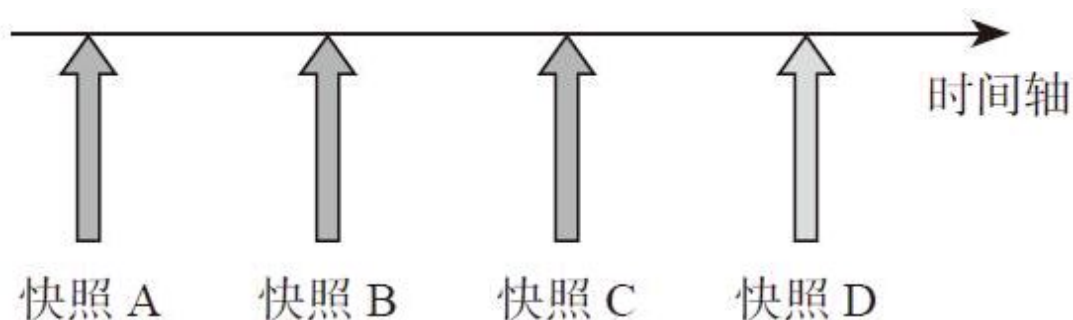


图4-45 定期给SSD拍照

假设图4-45中，在做完快照C后，做下一个快照D之前，SSD在X处发生了异常掉电，如图4-46所示。

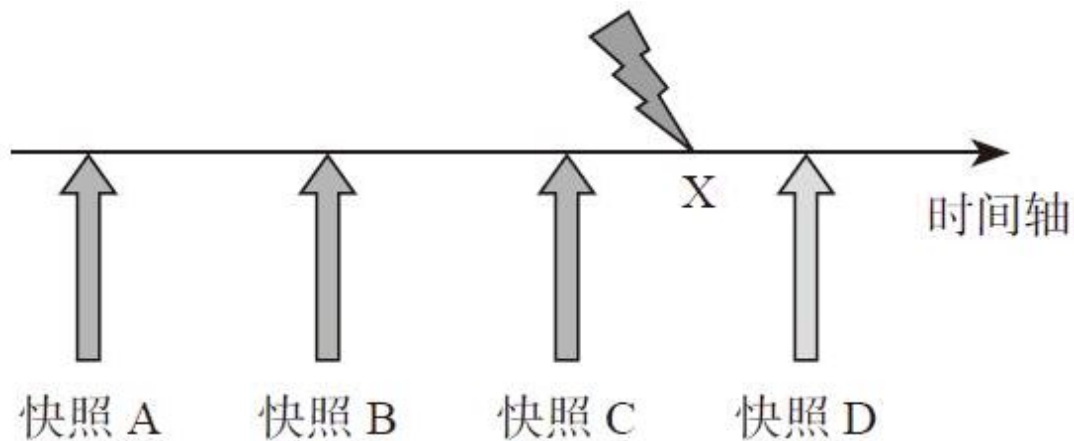


图4-46 异常掉电发生在快照C后

重上电，SSD可以从闪存中读取到最新的快照信息，即快照C。由于异常掉电，从快照C处到X处新产生的映射关系丢失。由于之前绝大多数的映射关系都被快照C保存，因此需要重建的映射关系仅仅是快照C之后产生的映射关系，这部分关系的恢复，仅需扫描一些局部的物理空间，因此，相对全盘扫描，映射表重建速度大大加快。

4.7 坏块管理

4.7.1 坏块来源

坏块来源主要包括:

- 出厂坏块 (Factory Bad Block) : 闪存从工厂出来, 就或多或少的有一些坏块。

- 增长坏块 (Grown Bad Block) : 随着闪存的使用, 一些初期好块也会变成坏块。变坏的原因, 主要是擦写磨损。

4.7.2 坏块鉴别

闪存厂商在闪存出厂时，会对出厂坏块做特殊标记。一般来说，刚出厂的闪存都被擦除，里面的数据是全0xFF。但是对坏块来说，闪存厂商会打上不同的标记。拿TOSHIBA某型号闪存来说，它是这样标记出厂坏块的，如图4-47所示。

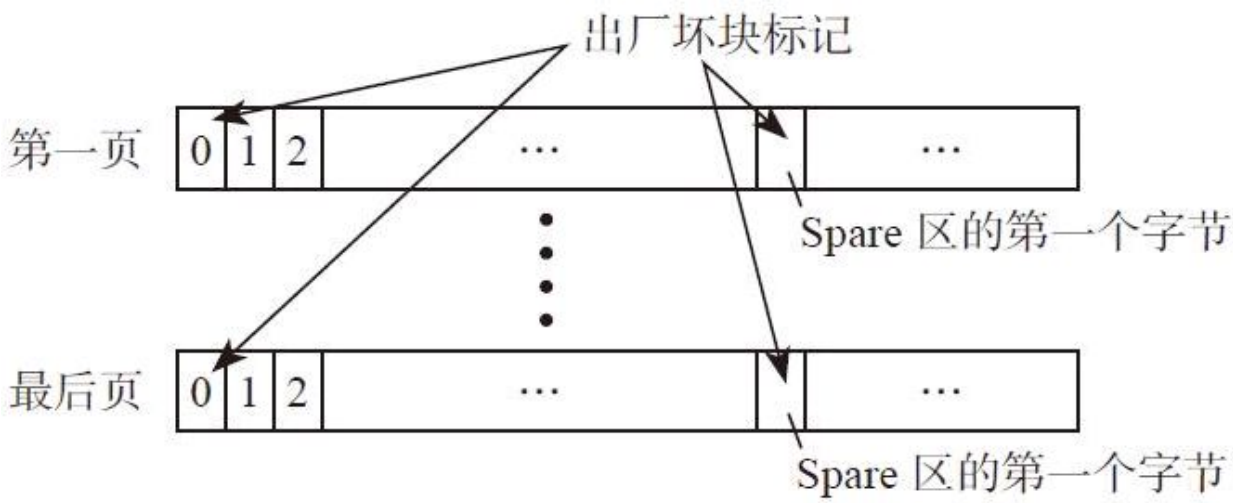


图4-47 出厂坏块标记示意图

它会在出厂坏块的第一个闪存页和最后一个闪存页的数据区第一个字节和Spare区第一个字节写上一个非0xFF的值。

用户在使用闪存的时候，首先应该按照闪存文档，扫描所有的闪存块，把坏块剔除出来，建立一张坏块表。还是拿上面的闪存来说，TOSHIBA建议按照下面的流程来建立坏块表（见图4-48）。

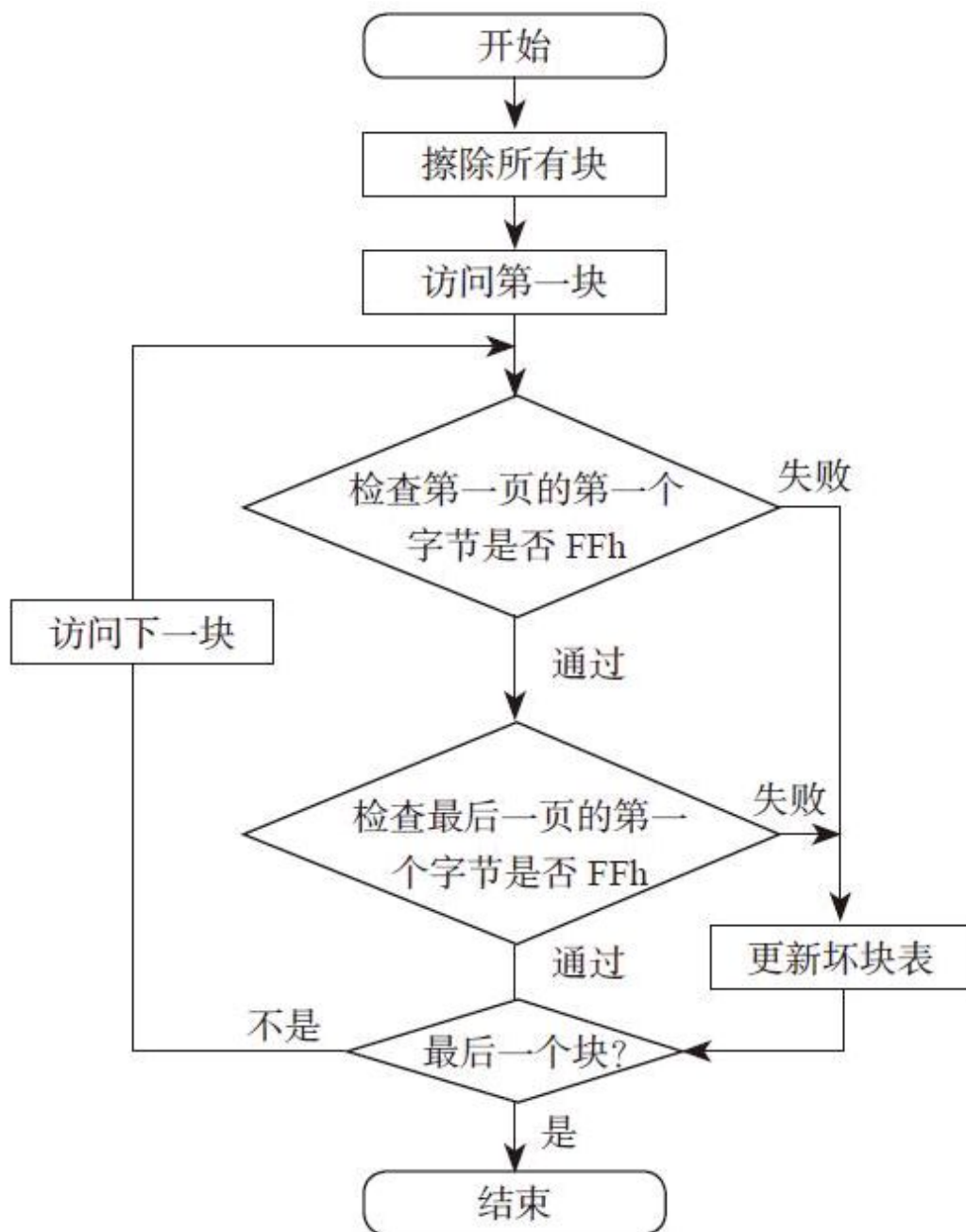


图4-48 根据出厂坏块标记建立坏块表流程图

还有些闪存厂商，它会把坏块信息存储在闪存内部某个地方（掉电不丢失），用户在建立坏块表的时候，没有必要扫描所有的闪存块来识别坏块，只需读取闪存的那个特定区域。比如Micron，它的闪存内部有个叫OTP（One Time Programming）的区域，出厂坏块信息可以存在里面。

对增长坏块而言，它的出现会通过读写擦等操作反映出来。比如读到UECC（Uncorrectable Error Correction Code，数据没有办法通过ECC纠错恢复）、擦除失败、写失败，这都是一个坏块出现的症状。用户应该把这些坏块加入坏块表，不再使用。

4.7.3 坏块管理策略

一般有两种策略管理坏块，一是略过（Skip）策略，二是替换（Replace）策略。

1.略过策略

用户根据建立的坏块表，在写闪存的时候，一旦遇到坏块就跨过它，写下一个Block。

SSD的存储空间是闪存阵列，一般有几个并行通道，每个通道上连接了若干个闪存。以图4-49为例，该SSD有四个通道，每个通道上挂了一个闪存Die。

		Die 0		Die 1		Die 2		Die 3
未写块								
坏块								
		A		B		C		D
已写块								
		通道 0		通道 1		通道 2		通道 3

图4-49 略过坏块B写数据

SSD向四个Die依次写入。假设Die 1上有个Block B是坏块，若固件采取坏块略过策略，则写完Block A时，接下来便会跨过Block B写到Die 2的Block C上面去。

2.替换机制

与略过策略不同，当某个Die上发现坏块时，它会被该Die上的某个好块替换。用户在写数据的时候，不是跨过这个Die，而是写到替换块上面去。采用此策略，除正常用户使用的闪存块，还需额外保留一部分好的闪存块，用于替换用户空间的坏块。整个Die上闪存块就划分为两个区域：用户空间和预留空间，如图4-50所示。

还是以上面的情况为例：用户写入数据时，当碰到坏块B，它不会略过Die 1不写，而是写入到Block B的替换者Block B'上面去。

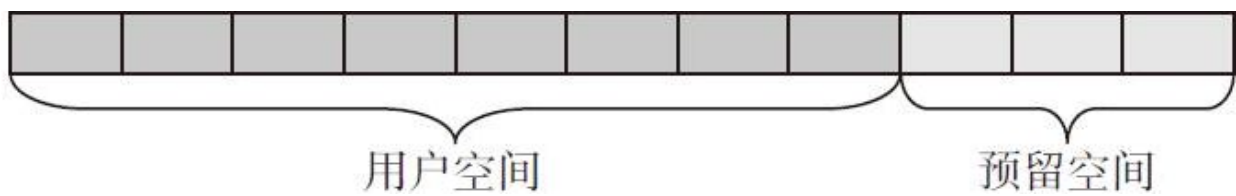


图4-50 闪存空间逻辑上分为用户空间和预留空间

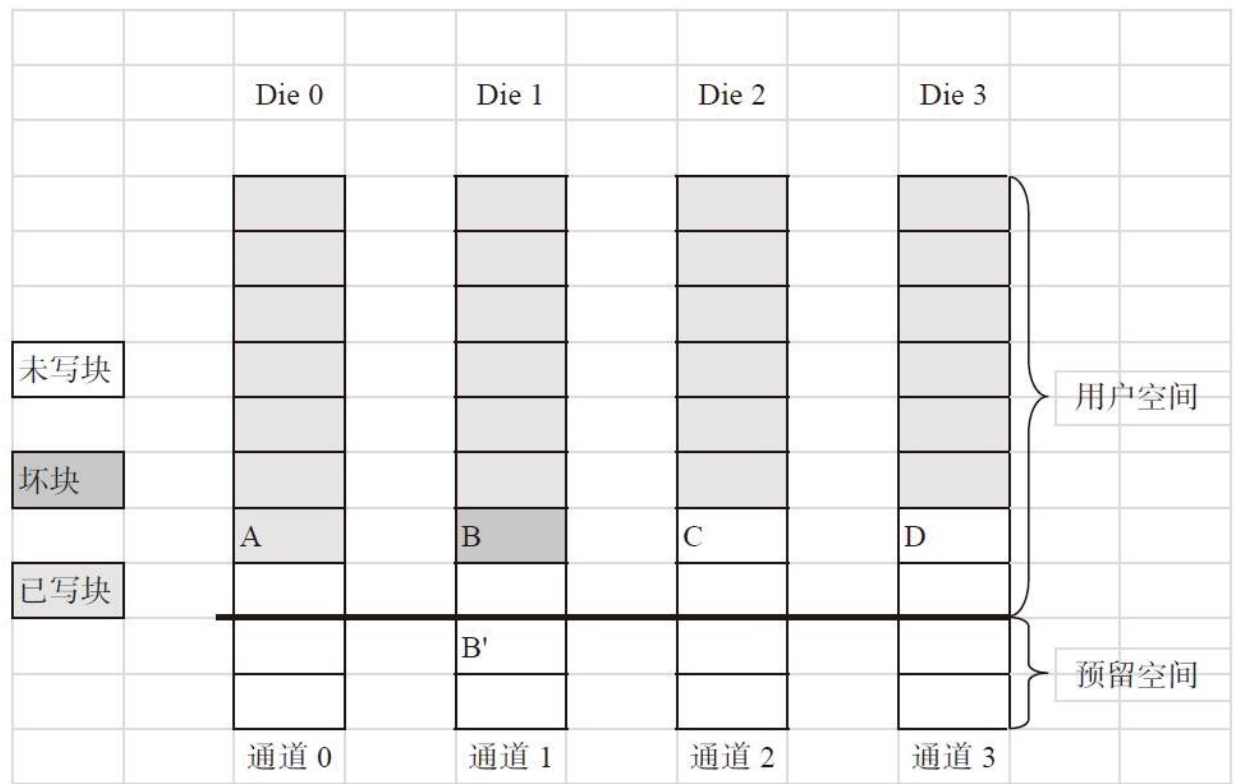


图4-51 用好块替换坏块后写入

采用替换策略，SSD内部需维护一张重映射表（Remap Table）：坏块到替换块的映射，比如图4-51的 $B \rightarrow B'$ 。当SSD需要访问Block B时，它需要查找重映射表，实际访问的物理Block应该是B'。

我们看看两者策略的优劣。

略过策略的劣势在于性能不稳定。以4个Die为例，略过策略可能导致Die的并行度在1和4个Die之间，而替换策略并行度总是4个Die，毋庸置疑，前者性能表现不如后者。但替换策略有木桶效应，如果某个Die质量比较差，则整个SSD可用的闪存块则受限于那个坏的Die。

4.8 SLC cache

SLC相对MLC和TLC来说，有更好的读写性能和更长的寿命。下面是SLC、MLC和TLC在性能和寿命（Endurance）上的一个直观对比，如表4-10所示（不同制程和不同商家的闪存，参数不尽相同，数据仅供参考）。

表4-10 SLC、MLC和TLC寿命和性能比较

闪存类型	SLC	MLC	TLC
每单元比特数	1	2	3

（续）

闪存类型	SLC	MLC	TLC
擦写次（次）	约 10 万	约 5000	约 1000
读时间（μs）	约 25	约 50	约 75
写时间（μs）	约 300	约 600	约 900
擦除时间（μs）	约 1500	约 3000	约 4500

由于SLC有速度优势，因此有些SSD拿它来做Cache使用，让SSD具有更好的突发性能（Burst Performance）。

这里所说的SLC Cache，不是说单独拿SLC闪存来做Cache，而是把MLC或者TLC里面的一些闪存块配置成SLC模式来访问，而这个特性一般的MLC或者TLC都是支持的。SLC模式下的闪存块，相比MLC或者TLC模式下的闪存块，更快更耐写，可以用来做Cache。

除了性能，SLC还有更好的耐写性，寿命更长。

使用SLC Cache的出发点，主要有以下几点：

- 1) **性能考虑：** SLC性能好，用户数据写到SLC比直接写到MLC或者TLC上快很多。
- 2) **防止Lower Page数据被带坏：** 用户数据写到SLC，不存在写Upper Page或者Extra Page带坏Lower Page数据的可能。
- 3) **解决闪存的缺陷：** 比如有些MLC或者TLC的闪存块，如果没有写满，然后去读的话，可能会读到ECC错误，而对SLC模式下的闪存

块，就没有这个问题。

4) 更多的数据写入量：SLC更耐写。

一般只有消费级SSD或者移动存储（比如eMMC、UFS等）使用SLC Cache，因为使用SLC Cache具有更好的突发性能；对企业级SSD来说，它追求的是稳态速度，它不希望SSD一下子速度飙升（写SLC），然后一下子速度急剧下降（写TLC）。

另外，消费级SSD和移动存储产品一般都没有电容保护，使用SLC Cache能保证Lower Page数据不丢失；而企业级SSD一般都配有电容，能保证闪存正常写入，它不存在Lower Page数据被带坏的问题，所以没有必要采用SLC Cache这种手段来保护数据。

SLC Cache写入策略有：

- 强制SLC写入：用户写入数据时，必须先写入到SLC闪存块，然后通过GC搬到MLC或者TLC闪存块；

- 非强制SLC写入：用户写入数据时，如果有SLC闪存块，则写入到SLC闪存块，否则直接写到MLC或者TLC闪存块。

强制写入策略能保护Lower Page数据，而后者不能。非强制SLC写入策略，具有更好的后期写入性能，因为在SLC闪存块耗尽的情况下，用户数据直接写入到MLC或者TLC；而对强制写入SLC策略来说，它一方面要把SLC的数据搬到MLC或者TLC，以腾出SLC空间供新用户数据的写入，同时又要将用户数据写入到SLC，性能肯定比只写MLC或者TLC慢。

在这里可能有的读者有疑惑，强制写入SLC策略，SLC数据最后都要搬到MLC或者TLC，所以还是存在直接写MLC或者TLC的事实，也就是还是存在Lower Page数据被带坏的可能。是的，没错，做GC（数据搬运）是有这个问题。但是，如果我们在目标闪存块没有被写满前，不把源闪存块擦除，这样即使Lower Page数据被带坏，它还是能通过读源闪存块恢复数据，是不是？

根据SLC闪存块的来源，有以下几种SLC Cache办法。

- 1) 静态SLC Cache：拿出一些Block专门用做SLC Cache；

2) 动态SLC Cache: 所有的MLC或者TLC都有可能挑来当SLC Cache, SLC和TLC不分家;

3) 两者混合: 即既有专门的SLC闪存块, 还能把其他通用闪存块拿来当SLC Cache。

4.9 RD&DR

RD指的是Read Disturb，DR指的是Data Retention。两者都能导致数据丢失，但原理和固件处理方式都不一样，下面分别介绍。

1.RD

对一个闪存块来说，每次读其中的一个闪存页，都需要在其他字线（Wordline）上加较高的电压以保证晶体管导通。对这些晶体管来说，有点像在做轻微的“写入（Program）”，长此以往，由于电子进入浮栅极过多，从而导致比特翻转： $1 \rightarrow 0$ 。当出错比特数超出ECC的纠错能力时，数据就会丢失。这就是RD的原理，更详细的内容可参看本书其他章节。RD为了读某个闪存页的数据，却要别的闪存页遭受损失，实在是有些损人利己。

由于每次都是很轻微的写入，要使存储单元数据发生变化，不是一朝一夕的事情，而是长期积累的结果。因此，如果我们能保证某个闪存块读的次数低于某个阈值，在比特发生翻转之前（或者翻转的比特低于某个值时），就对这个闪存块上的数据进行一次刷新：把闪存块上的数据搬到别的闪存块上（或者先搬到别的闪存块上，然后擦除原闪存块后，再复制回来），防患于未然，这样就能解决RD导致数据丢失的问题。

因此，FTL应该有记录每个闪存块读次数的一张表：每读一次该闪存块，对应的读次数加1。当FW检测到某个闪存块读的次数超过某个阈值，就刷新该闪存块。当数据写到新的闪存块后，读次数归零，一切重新开始。每个闪存块的读次数，掉电时应该保存到闪存上，重新上电时，再加载它们。

事实上，当某个闪存块上的读次数超出阈值时，上面的数据翻转可能并没有超过很多（可设阈值），这种情况就没有必要立刻刷新。毕竟，刷新带来的读数据和写数据，需要耗时间和擦写次数，对性能和闪存寿命有影响。因此，有些FTL为避免“过”刷新，可能会在读次数超过阈值后，先检测比特翻转数，然后决定是否真正需要刷新，如果不需要立刻刷新，会重新设置一个更大的阈值，待下次读的次数达到新阈值后，重复之前的操作。

关于读阈值，过去的FTL在SSD的整个生命周期中，都是用一个固定的值，这种处理简单粗暴，很不科学（但固件实现简单）。其实，RD与闪存的年龄有关：年龄越大（PE越大），对RD的免疫力越低。因此，对阈值的设定，采用动态的才是合理的，即对不同的PE，读阈值应该不同。具体来说，PE越大，读阈值应该越小。

关于刷新动作，有Block（阻塞）和Non-block（非阻塞）两种处理方式。所谓阻塞方式，就是固件把其他事情都放在一边，专门处理闪存块的刷新；所谓非阻塞方式，就是闪存块的刷新与其他操作同时进行（Interleave操作）。前者处理方式劣势明显，那就是带来很长的命令时延：在处理闪存块的刷新的时候，就不能执行读写操作，导致读写推后。随着闪存块尺寸的增大，这种处理方式的劣势越发凸显。所以，现在的FTL一般都采用非阻塞的刷新处理方式。

RD就说到这里，我们再说说DR。

2.DR

中国有句古话，就是天下没有不透风的墙。用到闪存上，就是没有电子穿越不了的绝缘材料。绝缘氧化层把存储在浮栅极的电子关在里面，但是，随着时间的推移，还是有电子从里面跑出来。当跑出来的电子达到一定数量时，就会使存储单元的比特发生翻转：0→1（注意，RD是使1翻转为0），当出错比特数超出ECC的纠错能力，数据就丢失。这就能解释为什么你的固态硬盘如果很长时间不用，可能就启动不了，或者启动很慢（固件需要处理由于DR引起的数据错误）的现象了。

问题来了，为什么SSD长久不用数据就会丢失，而经常使用却不会呢？原因是FW或者FTL立功了。针对DR这个问题，稍微好一点的SSD，FTL都会有相应的处理。怎么处理呢？FTL在SSD上电或者平时运行时，每隔一段时间对闪存空间进行扫描，当发现比特翻转超出一定阈值时，跟RD处理一样，进行数据刷新，这样就能避免数据彻底丢失。SSD如果常年不上电，FTL根本就没有机会执行这些操作，只能眼睁睁地看着电子流失。

4.10 Host Based FTL

按照FTL放在哪里划分，SSD有Host Based FTL和Device Based FTL两种模式。

顾名思义，Host Based把FTL放在主机驱动程序中，Device Based则是把FTL放在SSD主控内部。大部分企业级SSD和几乎全部消费级SSD都是Device Based，SSD主控芯片做了包括FTL在内的所有控制工作。也有一些企业级SSD采用了Host Based FTL，像垃圾回收、磨损平衡、坏块管理等都放在主机驱动程序中完成，这种模式的优点是可以实现差异化，典型产品是FusionIO。

4.10.1 Device Based FTL的不足

图4-52所示是两种模式的架构对比。看得出来，从逻辑上来说，一个完整的Device Based SSD系统可以分为三块：

1) 主机驱动：为应用程序提供读写接口；和板载控制器通过NVMe等协议进行交互，完成应用程序的读写命令。

2) 板载控制器：

- 通过SATA、NVMe等协议，接收主机发送的命令并执行。

- 管理SSD，实现FTL垃圾回收、磨损平衡等算法。

- 控制和实现闪存时序。

3) 闪存阵列：存储介质。

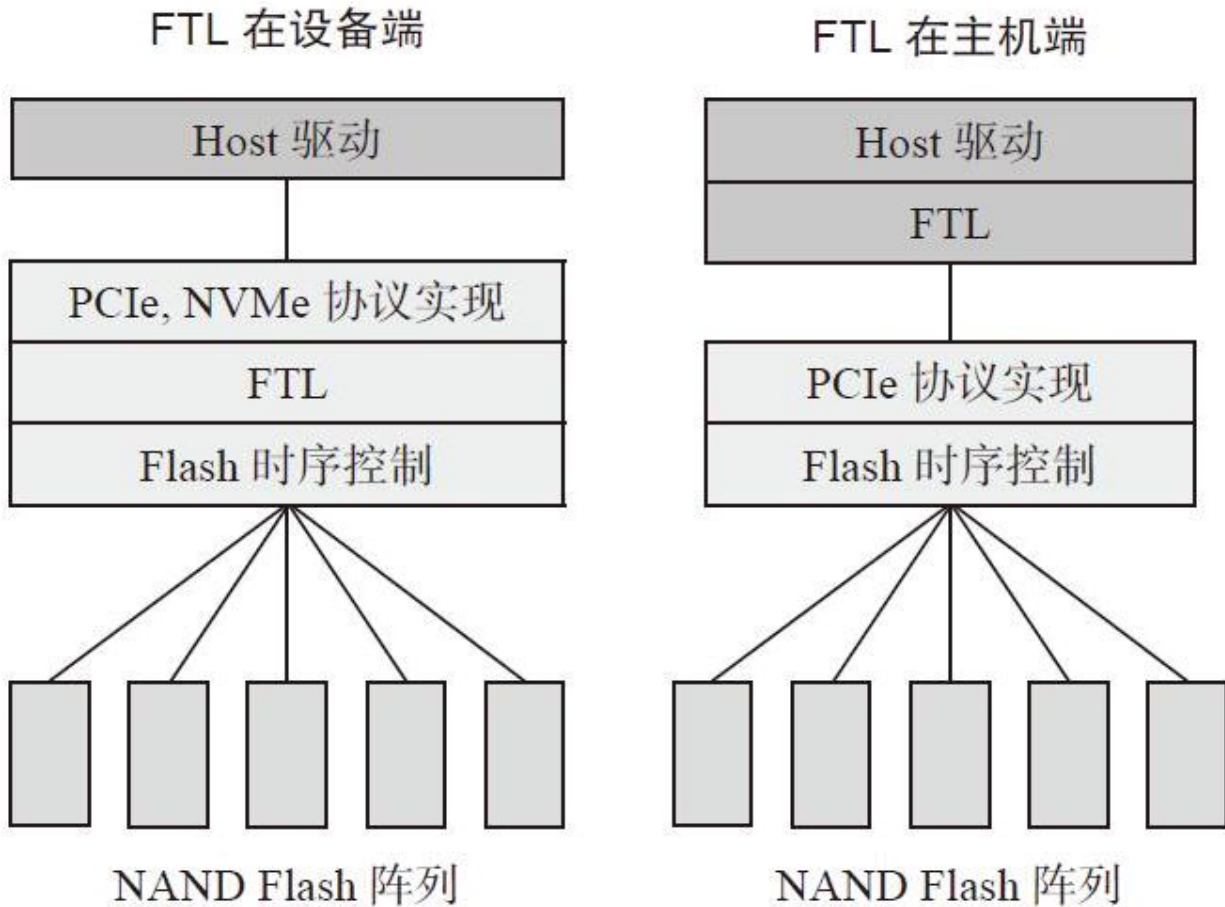


图4-52 Host Based FTL和Device Based FTL架构比较

Device Based是个通用的架构，在SATA、NVMe等协议的广泛普及下，产品越来越标准化。CPU制造商提供PCIe或者SATA支持，主板和服务商制造商为SSD提供接口和槽位，操作系统开发商提供SSD标准化驱动程序，SSD制造商只需要制造出符合SATA、SAS或NVMe标准的SSD就可以出货了。

大家分工合作，互不干扰，一切都看起来都很完美。在厂商的立场上确实很完美，但对用户来说就不完美了。SSD之所以是一场存储革命，是因为它实在是不同于机械硬盘。在HDD时代，用户只需要对着每个扇区写数据就可以了，不管是什么应用程序，都得按这个规矩来。SSD就不一样，它包含了很多闪存芯片，这些芯片可以并行读写，所以有些用户希望能针对自己的应用特点去直接管理闪存内部资源，达到更高的效率和性能。

总体来说，Device Based存在以下缺点：

- FTL架构通用，不能针对具体应用做定制化。

- 控制器芯片功能复杂，设计难度大，研发成本高。

- 闪存更新很快，一般每年闪存厂商都会推出新一代产品，有新的使用特性，需要控制器芯片做出修改，但是芯片改版成本很高。

- 企业级应用需要高性能、大容量，通用控制器芯片支持的最大性能和容量有限制。

- 企业级市场需求多种多样，有些需求需要控制器提供特殊功能支持，这些是通用SSD主控芯片无法提供的。

为了解决这些问题，有些企业级SSD采用了Host Based方案。也有一些大型互联网公司，例如Google、Microsoft，还有百度等，自己研发Host Based SSD，针对自己的存储架构，开发驱动程序和控制器逻辑。

4.10.2 Host Based FTL架构

Host Based SSD一般的模式是把闪存的读写接口直接开放给驱动程序，这样驱动程序就能自行管理闪存内部资源。控制器大都采用可编程逻辑器件FPGA，功能比较简单，主要实现ECC纠错和闪存时序控制。

如图4-53所示，主机驱动直接管理闪存阵列，控制器只是起到ECC纠错算法和物理协议转换的作用。

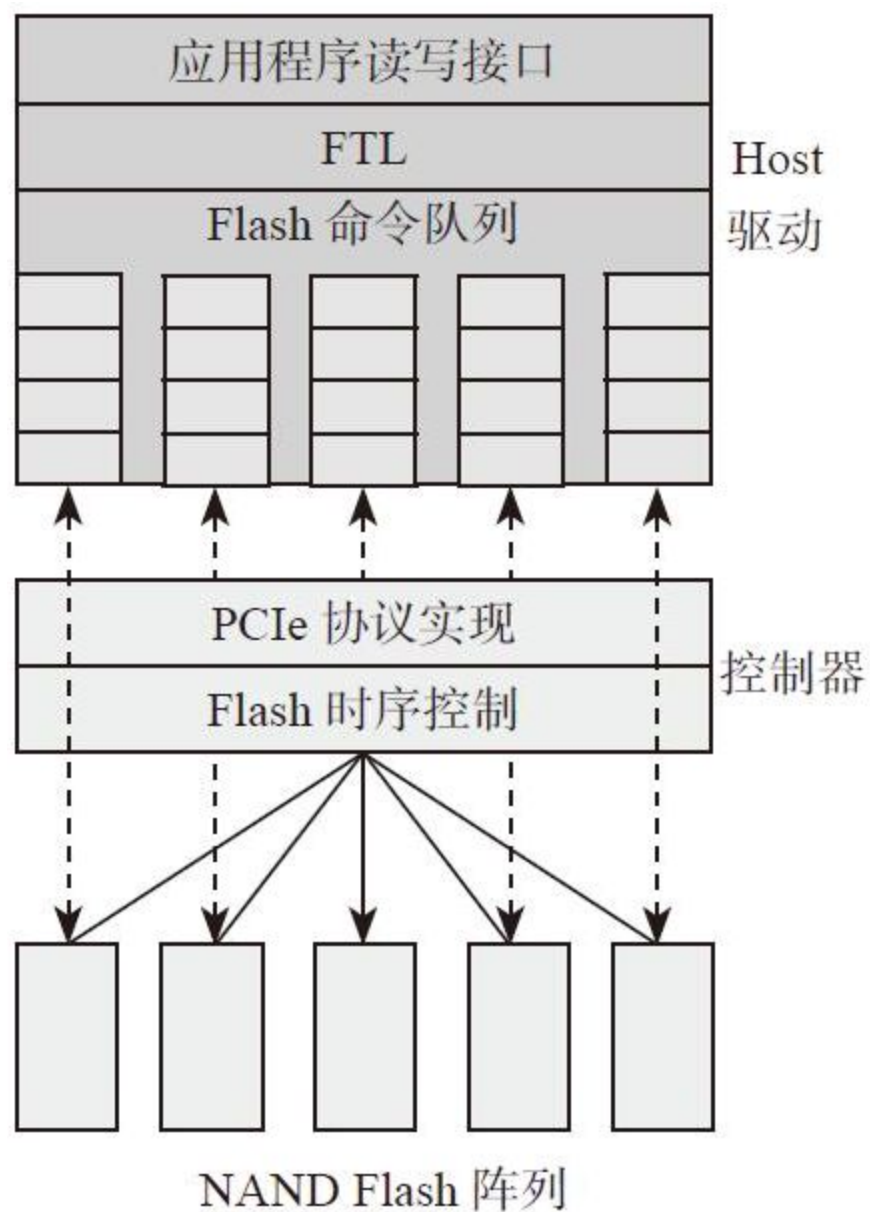


图4-53 Host Based FTL架构示意图

4.10.3 百度的软件定义闪存

在机械硬盘时代，硬盘的制造技术掌握在少数几家大公司手里，用户只能购买。但是进入SSD时代之后，硬盘的制造门槛没有那么高了，简单来说，SSD就是将闪存芯片和控制芯片组装起来，所以国内很多有技术实力的公司就想开发自己的SSD，例如华为、百度等。

百度、腾讯、阿里巴巴以及Google和Facebook等互联网巨头有着数量庞大的服务器，每家都是十万台级别，这注定了它们不能从存储厂商购买昂贵的服务器，只能自己研发廉价的服务器和存储设备来建设数据中心。这个存储设备也包括定制化的SSD。

百度的欧阳剑团队在国际著名的计算机体系结构学术会议ASPLOS'14上发表了一篇文章，介绍他们研发的软件定义闪存SDF（Software Defined Flash）。相比市场上销售的SSD，SDF主要的特点有：

1) 没有垃圾回收。SDF的使用者使用闪存块大小的整数倍为单位来写数据（比如8MB），所以每个闪存块里面不会有垃圾，或者整体都是垃圾，写之前直接擦除就可以了。这样的好处有：

- SSD内部不用做垃圾回收，读写带宽得到提高。
- 不需要预留空间，释放出20%的额外空间。
- 没有内部搬移数据产生的写操作，闪存没有了写放大，寿命延长。



图4-54 SDF板

2) 没有闪存级RAID。SSD内部其实是闪存阵列，所以为了数据安全性，很多企业级SSD会用闪存组成RAID组，用一块或几块闪存保存RAID数据。但是互联网公司的数据一般都有3个备份，所以不担心SSD内部数据丢失，因此，RAID是没有必要的。

3) FPGA作为控制芯片，功能很少：ECC、坏块管理、地址转换、动态磨损平衡。Virtex-5FPGA实现了PCIe接口和DMA，Spartan FPGA则是闪存控制芯片。

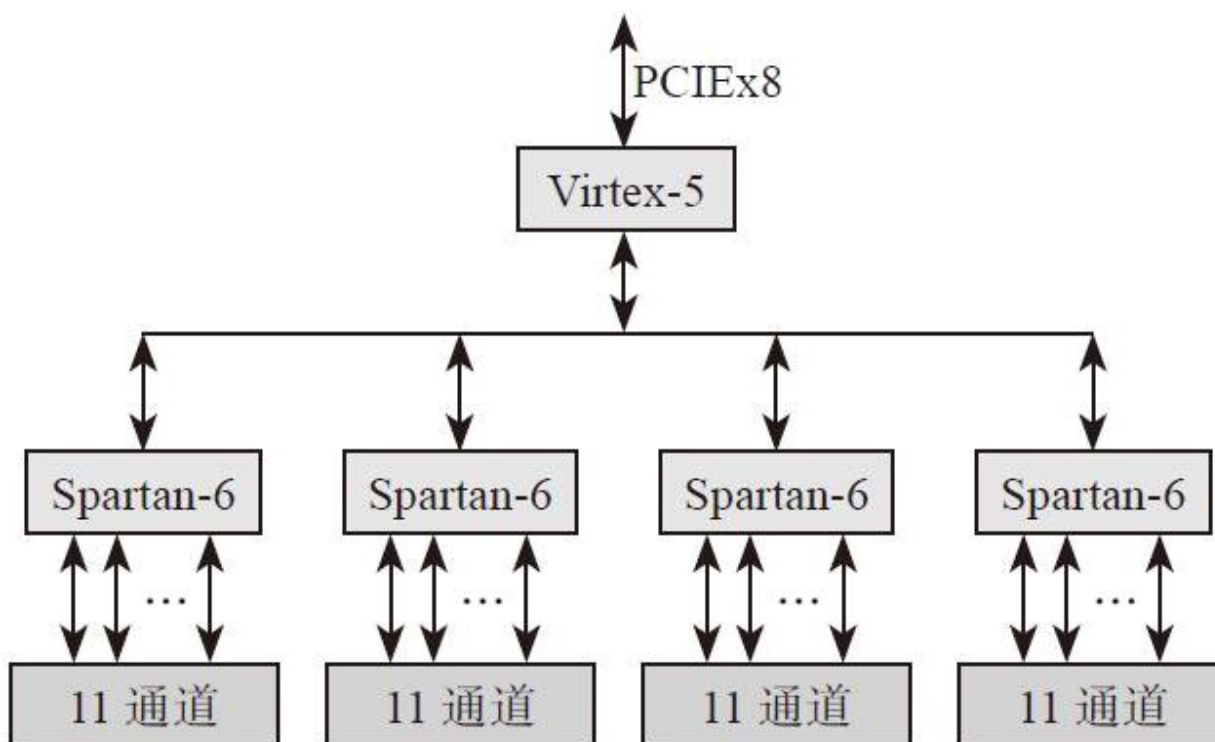


图4-55 SDF硬件架构图

4) SSD内部每个通道都向用户开放，由用户选择写哪个通道。

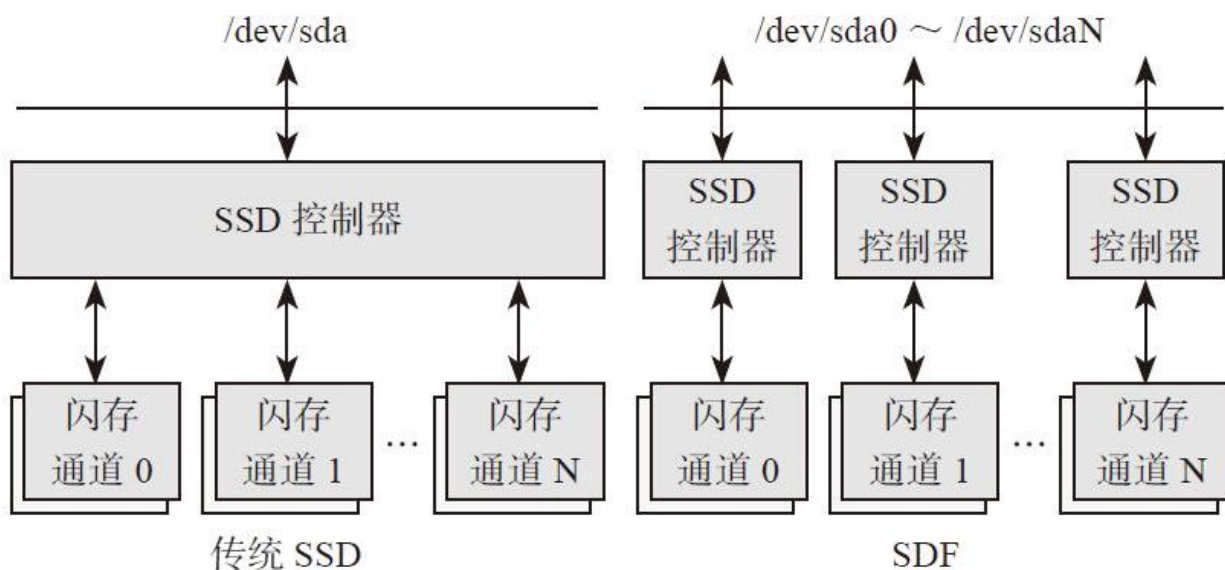


图4-56 SDF和传统SSD比较

5) 软件接口层非常简单，相比传统的Linux存储堆栈，省略了文件系统、块设备、IO调度、SATA协议等，用户直接通过IOCTRL（设备驱动程序中对设备的I/O通道进行管理的函数）来发同步的写命令到PCIe驱动，如图4-57所示。软件延迟从12 μ s缩减到2~4 μ s，这个时间只是花在PCIe中断处理上。

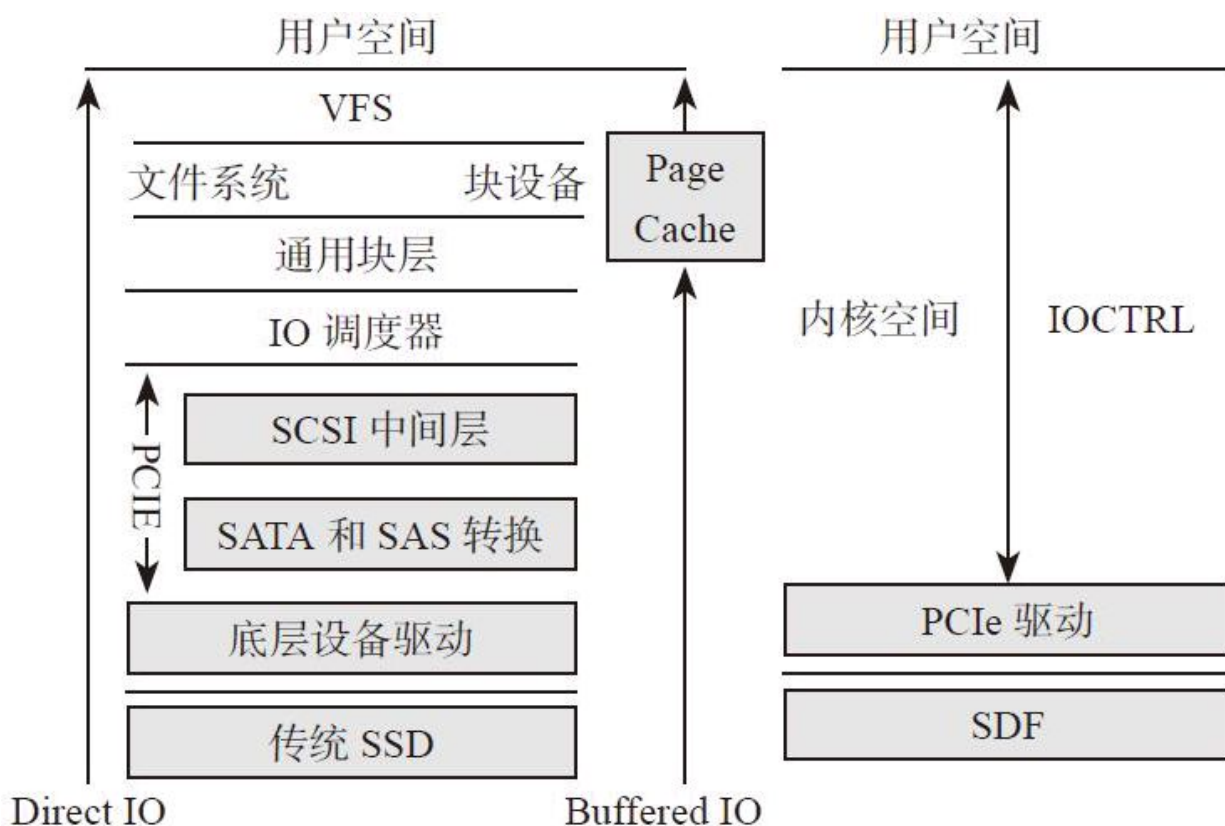


图4-57 SDF和传统SSD IO栈对比

SDF内部保存的数据是百度自己的日志文件系统数据，每个数据块大概8MB。

看得出来，百度的这个软件定义闪存针对自己的应用特点，仅仅保留了最关键的功能，SSD设计得非常精简，节约了大量的资源，同时延迟也很短。

FTL部分就讲到这儿，希望读者看完后有所收获。读者也可以关注SSDFans微信公众号和网站www.ssdfans.com，获取更多FTL和SSD相关知识。

第5章 PCIe介绍

5.1 从PCIe的速度说起

现在，SSD已经大跨步迈入PCIe时代。作为SSD的一项重要技术，我们有必要对PCIe有个基本的了解。

为什么SSD要用PCIe接口？因为它快，比SATA快。它究竟有多快？我们首先从PCIe接口的速度开始我们的PCIe之旅。

PCIe发展到现在，从PCIe 1.0、PCIe 2.0，到现在的PCIe 3.0，速度一代比一代快，如表5-1所示。

表5-1 PCIe各代的带宽

链接速度	× 1	× 2	× 4	× 8	× 12	× 16	× 32
Gen1 带宽 (GB/s)	0.5	1	2	4	6	8	16
Gen2 带宽 (GB/s)	1	2	4	8	12	16	32
Gen3 带宽 (GB/s)	2	4	8	16	24	32	64

2017年，PCIe4.0已经发布，但本章内容仅限于PCIe 3.0或更早版本。

从链接速度这一行我们看到×1、×2、×4.....这是什么意思？这是指PCIe连接的通道数（Lane）。就像高速公路一样，有单车道、2车道、4车道的（见图5-1），不过像8车道或者更多车道的公路不常见，但PCIe是可以最多有32个Lane的。

两个设备之间的PCIe连接，叫作一个Link，如图5-2所示。

如图5-2所示，A与B之间是个双向连接，车可以从A驶向B，同时，车也可以从B驶向A，各行其道。两个PCIe设备之间，有专门的发送和接收通道，数据可以同时往两个方向传输，PCIe Spec称这种工作模式为双单工模式（Dual-Simplex），可以理解为全双工模式。



图5-1 PCIe Lane类比高速公路通道

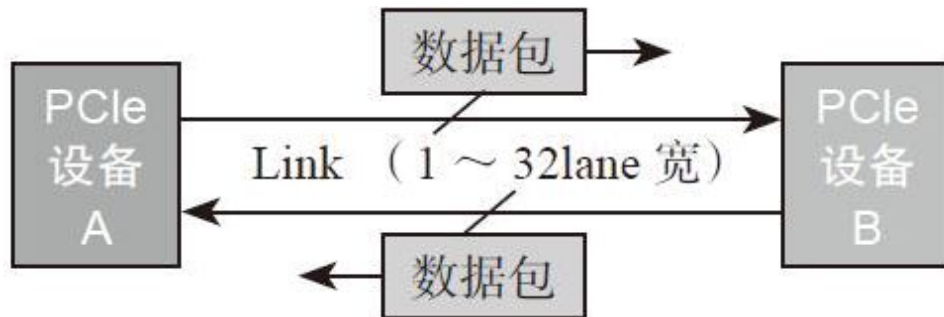


图5-2 PCIe Link的概念

SATA是什么工作模式呢？如图5-3所示。

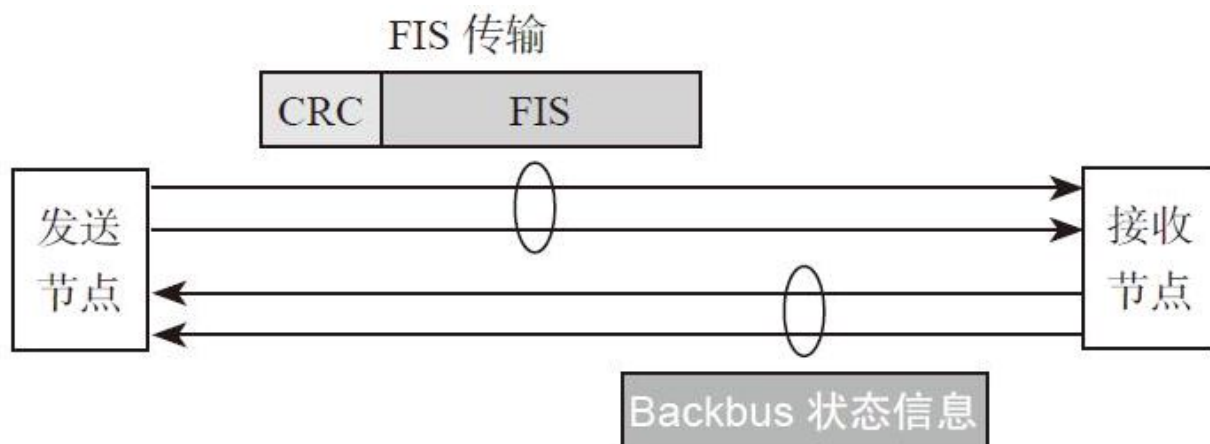


图5-3 SATA工作模式

和PCIe一样，SATA也有独立的发送和接收通道，但与PCIe工作模式不一样，同一时间，只有一条通道可以进行数据传输。也就是说，你在一条通道上发送数据，在另外一条通道上就不能接收数据，反之亦然。这种工作模式称为半双工模式。

PCIe犹如我们的手机，双方可以同时讲话，而SATA就是对讲机了，一个人在说话，另外一个人就只能听不能说。

回到表5-1，表中的带宽，比如PCIe3.0×1，带宽为2GB/s，是指双向带宽，即读写带宽。如果单指读或者写，该值应该减半，即1GB/s的读速度或者写速度。

我们来看看表里面的带宽是怎么算出来的。

PCIe是串行总线，PCIe1.0的线上比特传输速率为2.5Gbps，物理层使用8/10编码，即8bit的数据，实际在物理线路上是需要传输10bit的，多余的2bit用来校验。因此：

$$\text{PCIe1.0} \times 1 \text{ 的带宽} = (2.5\text{Gbps} \times 2 \text{ (双向通道)}) / 10 = 0.5\text{GB/s}$$

这是单条Lane的带宽，有几条Lane，那么整个带宽计算就是用0.5GB/s乘以Lane的数目。

PCIe2.0的线上比特传输速率在PCIe1.0的基础上翻了一倍，为5Gbps，物理层同样使用8/10编码，所以：

PCIe2.0×1的带宽=（5Gbps×2（双向通道））/10=1GB/s

同样，有多少条Lane，带宽就是1GB/s乘以Lane的数目。

PCIe3.0的线上比特传输速率没有在PCIe2.0的基础上翻倍，不是10Gbps，而是8Gbps，但物理层使用的是128/130编码进行数据传输，所以：

PCIe3.0×1的带宽=（8Gbps×2（双向通道）×
（128bit/130bit））/8≈2GB/s

同样，有多少条Lane，带宽就是2GB/s乘以Lane的数目。

由于采用了128/130编码，每128bit的数据，只额外增加了2bit的开销，有效数据传输比率增大，虽然线上比特传输率没有翻倍，但有效数据带宽还是在PCIe2.0的基础上实现翻倍。

这里值得一提的是，上面算出的数据带宽已经考虑到8/10或者128/130编码，因此，大家在算带宽的时候，没有必要再考虑线上编码的问题了。

和SATA单通道不同，PCIe连接可以通过增加通道数扩展带宽，弹性十足。通道数越多，速度越快。不过，通道数越多，成本越高，占用更多空间，还有就是更耗电。因此，使用多少通道，应该在性能和其他因素之间进行一个综合考虑。单考虑性能的话，PCIe最高带宽可达64GB/s，即PCIe 3.0×32对应的带宽，这是很恐怖的一个数据。不过，现有的PCIe SSD一般最多使用4通道，如PCIe3.0x4，双向带宽为8GB/s，读或者写带宽为4GB/s。

Intel SSD 750 参数		
容量	400GB	1.2TB
外形尺寸	2.5"15mm SFF-8639 or PCIe Add-In Card (HHHL)	
接口	PCIe3.0 × 4-NVMe	
控制器	Intel CH29AE41AB0	
NAND	Intel 20nm 128Gbit MLC	
顺序读	2200MB/s	2400MB/s
顺序写	900MB/s	1200MB/s
4KB 随机读	430k IOPS	440k IOPS
4KB 随机写	230k IOPS	290k IOPS
空闲功耗	4W	4W
读写功耗	9W/12W	10W/22W
加密支持	N/A	
耐写性	70GB Writes per Day for Five Years	

图5-4 Intel PCIe SSD 750规格书

在此，顺便来算算PCIe3.0×4理论上最大的4KB IOPS。PCIe3.0×4理论最大读或写的速度为4GB/s，不考虑协议开销，每秒可以传输4GB/4KB个4KB大小的IO，该值为1M，即理论上最大IOPS为1000k。因此，一个SSD，不管底层用什么介质，闪存还是3D XPoint，接口速度就这么快，最大IOPS是不可能超过这个值的。

PCIe是从PCI发展过来的，PCIe的“e”是express的简称，表示“快”。PCIe怎么就能比PCI（或者PCI-X）快呢？那是因为PCIe在物理传输上，跟PCI有着本质的区别：PCI使用并口传输数据，而PCIe使用的是串口传输。我PCI并行总线，单个时钟周期可以传输32bit或64bit，怎么就比不了你单个时钟周期传输1个bit数据的串行总线呢？

在实际时钟频率比较低的情况下，并口因为可以同时传输若干比特，速率确实比串口快，如图5-5所示。随着技术的发展，要求数据传输速率越来越快，要求时钟频率也越来越快，但是，并行总线时钟频率不是想快就能快的。

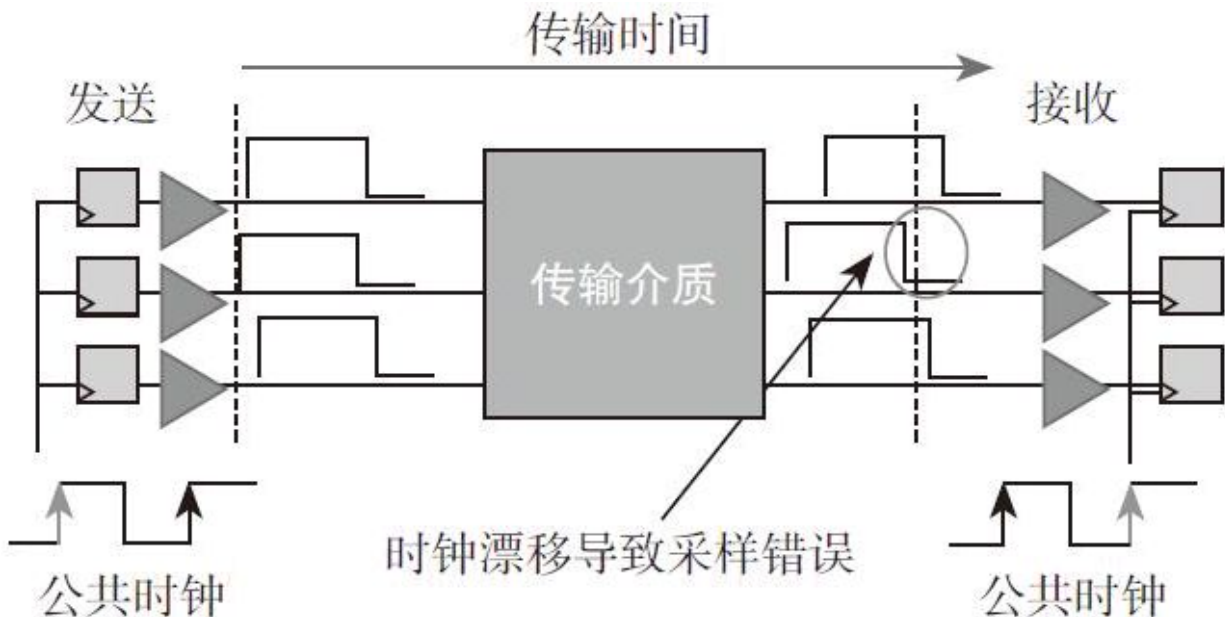


图5-5 并行传输时序

在发送端，数据在某个时钟沿传出去（左边时钟第一个上升沿），在接收端，数据在下个时钟沿（右边时钟第二个上升沿）接收。因此，要在接收端能正确采集到数据，要求时钟的周期必须大于数据传输的时间（从发送端到接收端的时间，**Flight Time**），受限于数据传输时间（该时间还随着数据线长度的增加而增加），因此时钟频率不能做得太高。另外，时钟信号在线上传输的时候，也会存在相位偏移（**Clock Skew**），影响接收端的数据采集。由于采用并行传输，接收端必须等最慢的那个bit数据到了以后，才能锁住整个数据。

PCIe使用串行总线进行数据传输就没有这些问题。它没有外部时钟信号，它的时钟信息通过8/10编码或者128/130编码嵌入在数据流，接收端可以从数据流里面恢复时钟信息，因此，它不受数据在线上传输时间的限制，导线多长、数据传输频率多快都没有问题。没有外部时钟信号，自然就没有所谓的相位偏移问题。由于是串行传输，只有一个bit传输，所以不存在信号偏移（**Signal Skew**）问题。但是，如果使用多条Lane传输数据（串行中又有并行），这个问题又回来了，因

为接收端同样要等最慢的那个Lane上的数据到达才能处理整个数据。不过，你不用担心，PCIe自己能解决好这个问题。

5.2 PCIe拓扑结构

计算机网络的拓扑结构是引用拓扑学中研究与大小、形状无关的点、线关系的方法，把网络中的计算机和通信设备抽象为一个点，把传输介质抽象为一条线，由点和线组成的几何图形就是计算机网络的拓扑结构。

计算机网络主要的拓扑结构有总线型拓扑、环形拓扑、树形拓扑、星形拓扑、混合型拓扑以及网状拓扑。

PCI采用的是总线型拓扑结构，一条PCI总线上挂着若干个PCI终端设备或者PCI桥设备，大家共享该条PCI总线，哪个人想说话，必须获得总线使用权，然后才能发言。如图5-6所示是一个基于PCI的传统计算机系统。

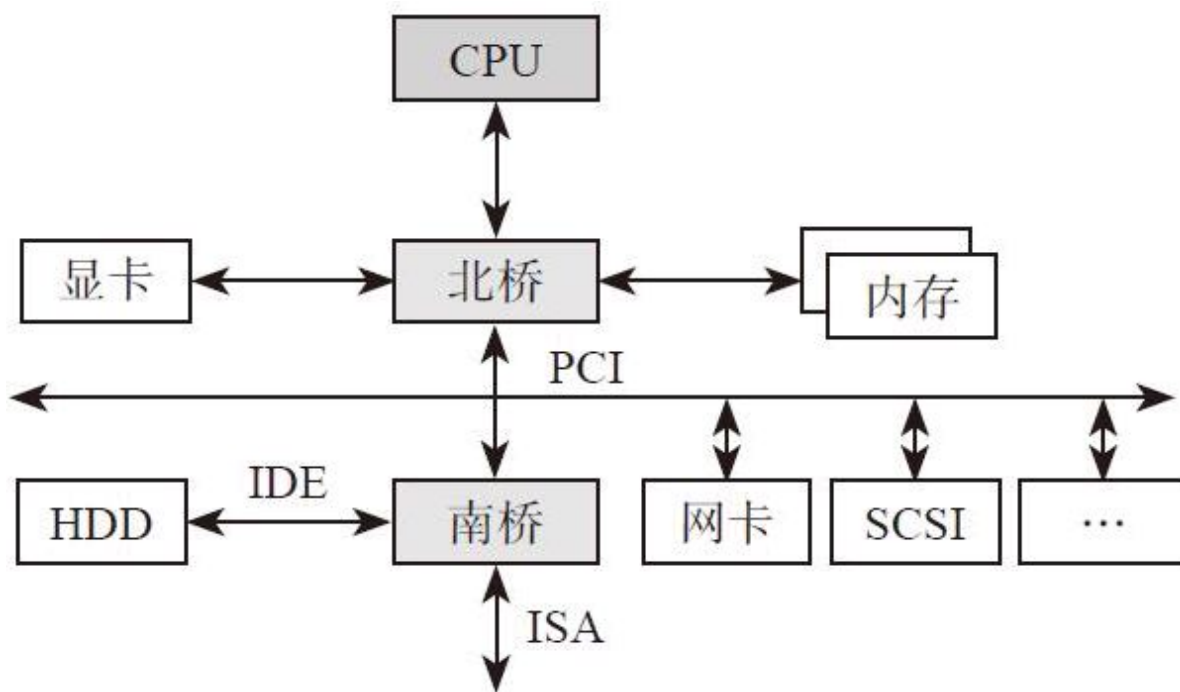


图5-6 基于PCI的传统计算机系统

北桥下面的那根PCI总线，挂载了以太网设备、SCSI设备、南桥以及其他设备，它们共享那条总线，某个设备只有获得总线使用权才能进行数据传输。

而PCIe则采用树形拓扑结构，一个简单而又典型的PCIe拓扑结构如图5-7所示。

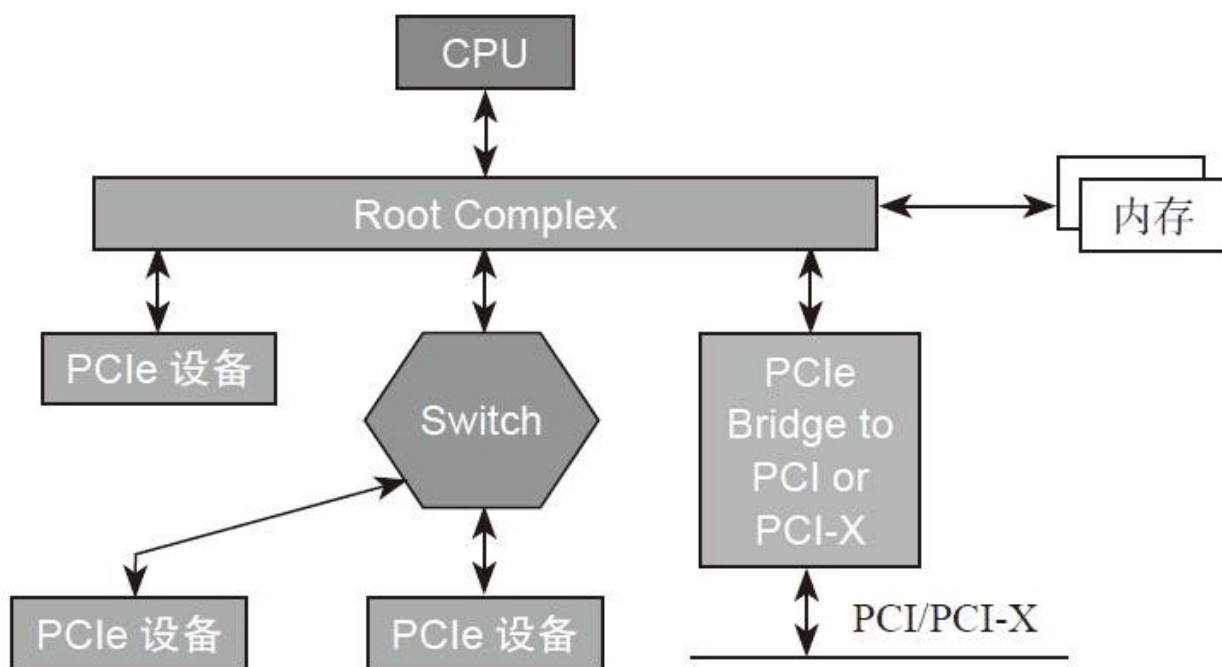


图5-7 基于PCIe计算机系统

整个PCIe拓扑结构是一个树形结构。Root Complex（RC）是树的根，它为CPU代言，与整个计算机系统其他部分通信，比如CPU通过它访问内存，通过它访问PCIe系统中的设备。

RC的内部实现很复杂，PCIe Spec也没有规定RC该做什么，不该做什么。我们也不需要知道那么多，只需清楚：它一般实现了一条内部PCIe总线（BUS 0），以及通过若干个PCIe bridge，扩展出一些PCIe Port，如图5-8所示。

PCIe Endpoint，就是PCIe终端设备，比如PCIe SSD、PCIe网卡等，这些Endpoint可以直接连在RC上，也可以通过Switch连到PCIe总线上。Switch用于扩展链路，提供更多的端口用以连接Endpoint。拿USB打比方，计算机主板上提供的USB口有限，如果你要连接很多USB设备，比如无线网卡、无线鼠标、USB摄像头、USB打印机、U盘等，USB口不够用，我会上网买个USB HUB用以扩展接口。

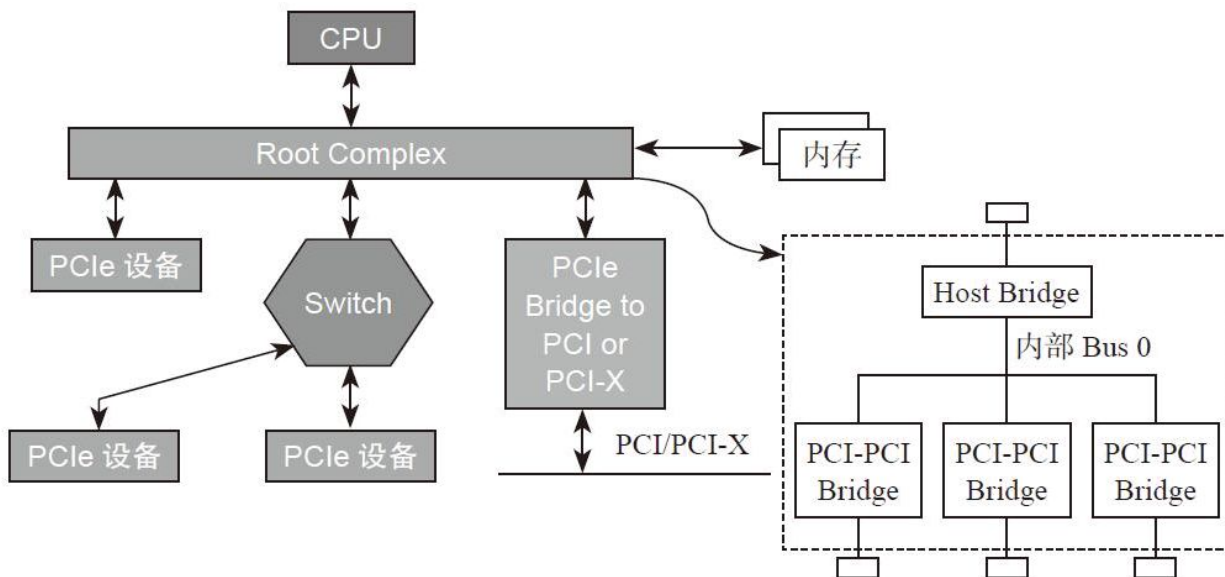


图5-8 Root Complex内部总线

Switch扩展了PCIe端口，靠近RC的那个端口，我们称为上游端口（Upstream Port），而分出来的其他端口，我们称为下游端口（Downstream Port）。一个Switch只有一个上游端口，可以扩展出若干个下游端口。下游端口可以直接连接Endpoint，也可以连接Switch，扩展出更多的PCIe端口，如图5-9所示。

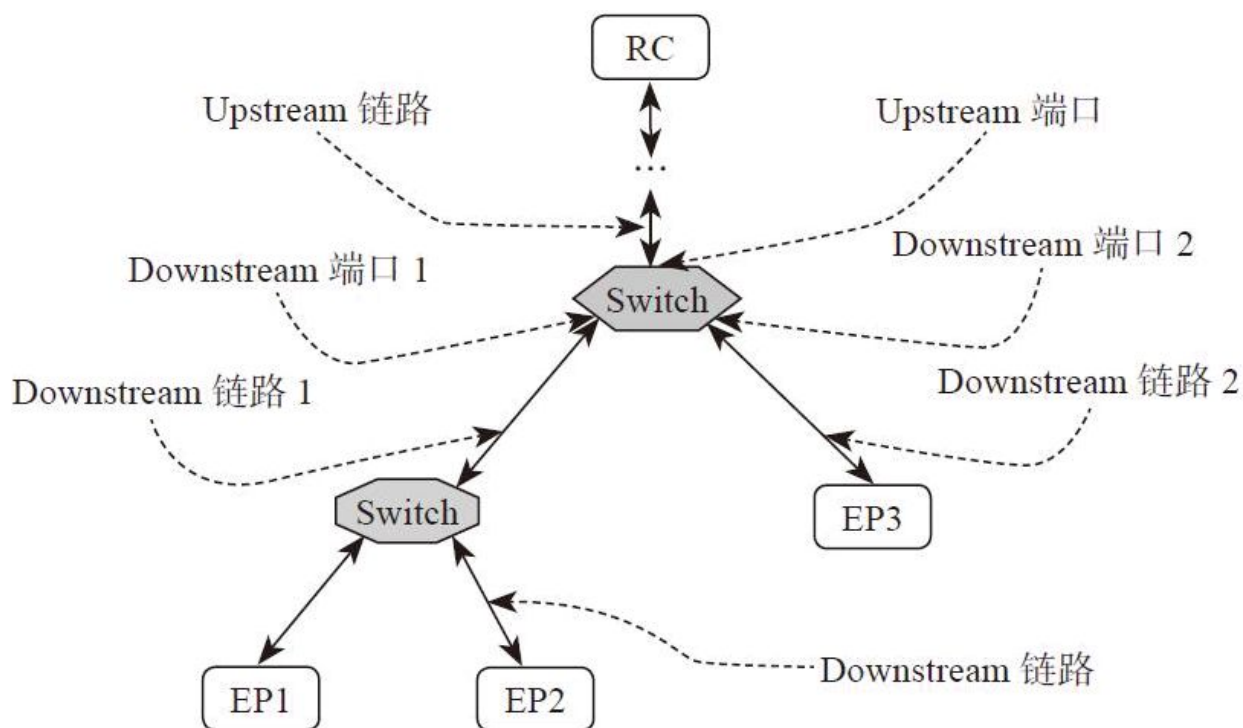


图5-9 PCIe Switch

对每个Switch来说，它下面的Endpoint或者Switch，都是归它管的。上游下来的数据，它需要甄别数据是传给它下面哪个设备的，然后进行转发；下面设备向RC传数据，也要通过Switch代为转发。因此，Switch的作用就是扩展PCIe端口，并为挂在它上面的设备（Endpoint或者Switch）提供路由和转发服务。

每个Switch内部，也是有一根内部PCIe总线的，然后通过若干个Bridge，扩展出若干个下游端口，如图5-10所示。

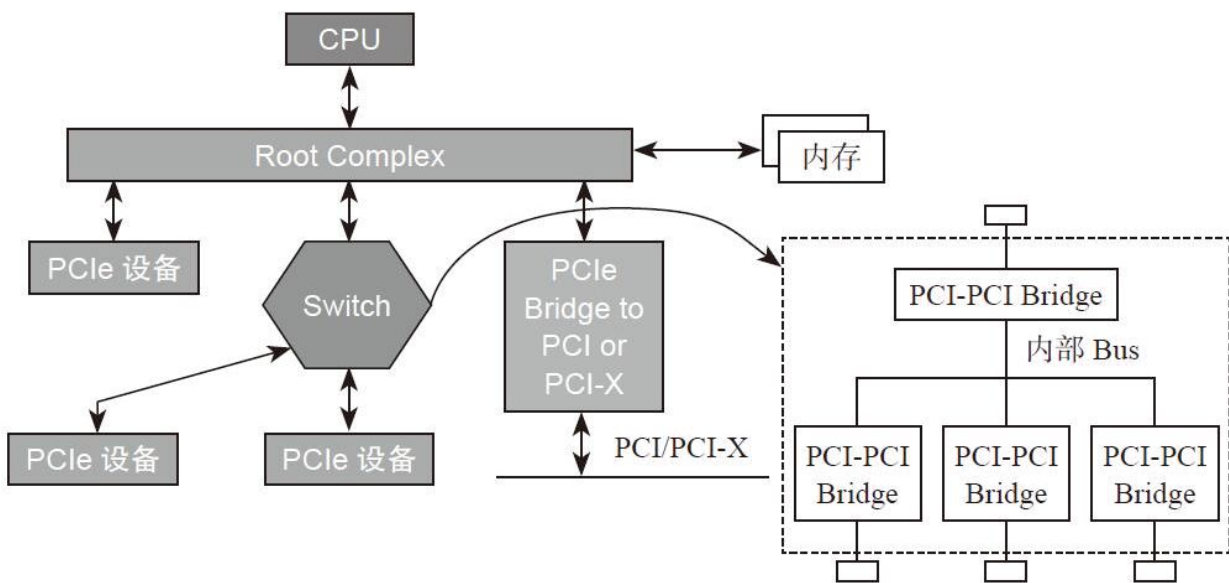


图5-10 Switch内部总线结构

最后小结一下：

PCIe采用的是树形拓扑结构，RC是树的根或主干，它为CPU代言，与PCIe系统其他部分通信，一般为通信的发起者。Switch是树枝，树枝上有叶子（Endpoint），也可节外生枝，Switch上连Switch，归根结底，是为了连接更多的Endpoint。Switch为它下面的Endpoint或Switch提供路由转发服务。Endpoint是树叶，诸如SSD、网卡、显卡等，实现某些特定功能（Function）。我们还看到有所谓的Bridge，用以将PCIe总线转换成PCI总线，或者反过来，不是我们要讲的重点，忽略之。PCIe与采用总线共享式通信方式的PCI不同，PCIe采用点对点（Endpoint to Endpoint）的通信方式，每个设备独享通道带宽，速度和效率都比PCI好。

需要指出的是，虽然PCIe采用点到点通信，即理论上任何两个Endpoint都可以直接通信，但实际中很少这样做，因为两个不同设备的数据格式不一样，除非这两个设备是同一个厂商的。通常都是Endpoint与RC通信，或者Endpoint通过RC与另外一个Endpoint通信。

5.3 PCIe分层结构

绝大多数的总线或者接口，都是采用分层实现的。PCIe也不例外，它的层次结构如图5-11所示。

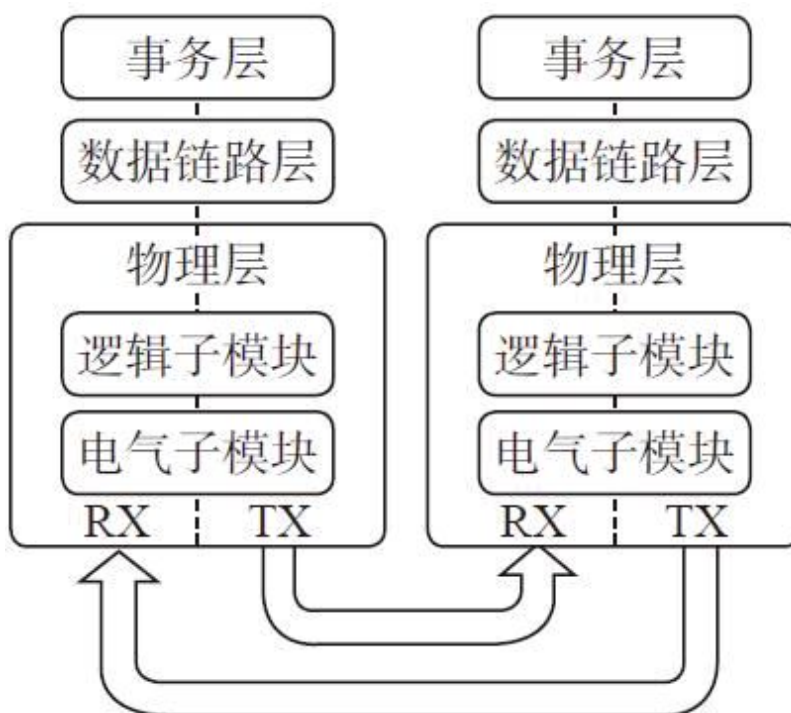


图5-11 PCIe分层结构

PCIe定义了下三层：事务层（Transaction Layer）、数据链路层（Data Link Layer）和物理层（Physical Layer，包括逻辑子模块和电气子模块），每层职能是不同的，但下层总是为上层服务的。分层设计的一个好处是，如果层次分得够好，接口版本升级时，硬件设计可能只需要改动某一层，其他层可以保持不动。

PCIe传输的数据从上到下，都是以数据包（Packet）的形式传输的，每层数据包都是有其固定的格式。

事务层的主要职责是创建（发送）或者解析（接收）TLP（Transaction Layer Packet）、流量控制、QoS、事务排序等。

数据链路层的主要职责是创建（发送）或者解析（接收）DLLP（Data Link Layer Packet）、Ack/Nak协议（链路层检错和纠错）、流控、电源管理等。

物理层的主要职责是处理所有的Packet数据物理传输，发送端数据分发到各个Lane传输（Stripe），接收端把各个Lane上的数据汇总起来（De-stripe），每个Lane上加扰（Scramble，目的是让0和1分布均匀，去除信道的电磁干扰EMI）和去扰（De-scramble），以及8/10或者128/130编码解码等。

这里先贴个这三层的细节图（见图5-12）。

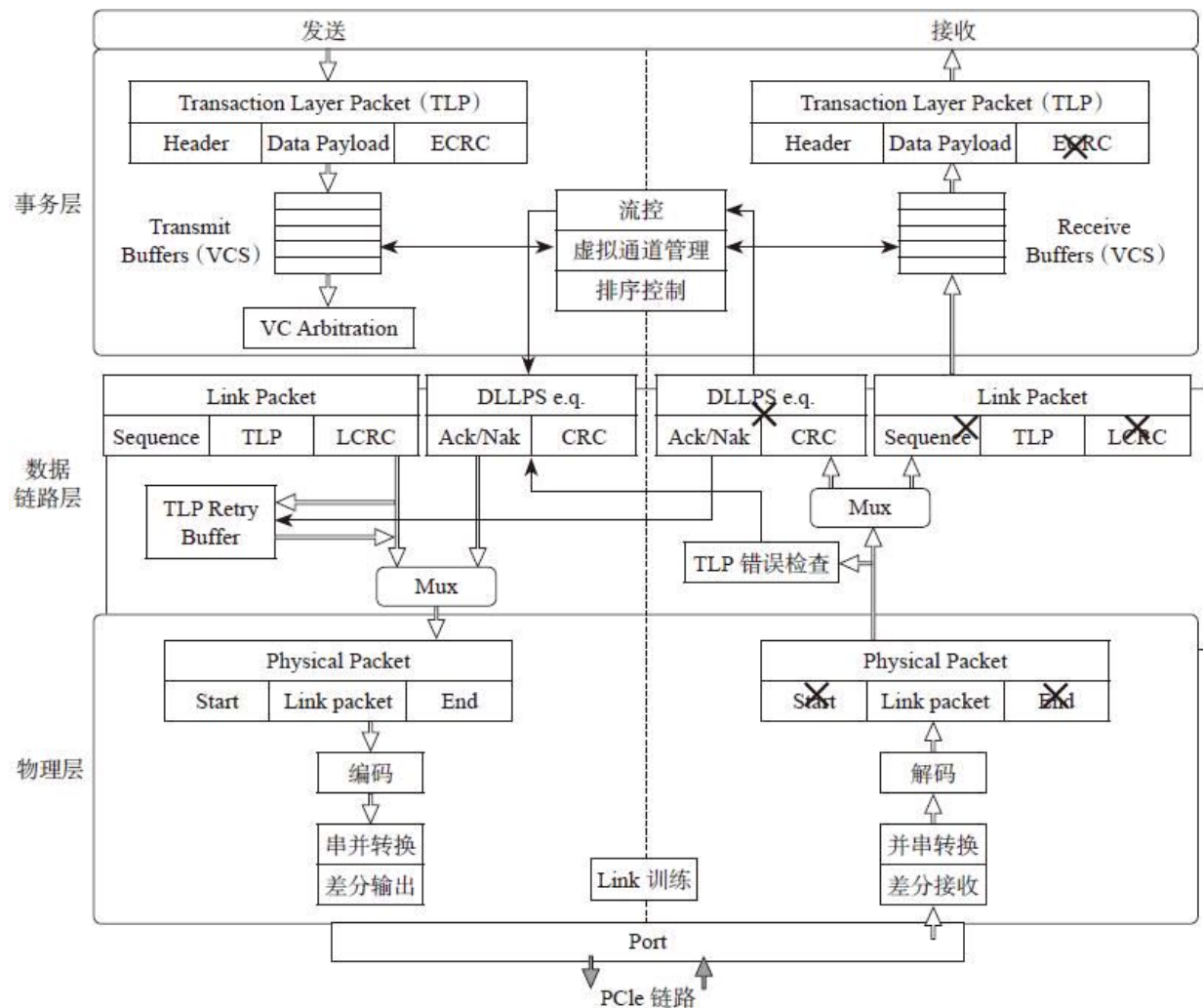


图5-12 PCIe各层次细节图

数据从上到下，一层层打包，上层打包完的数据，作为下层的原始数据，再打包。就像人穿衣服一样，穿了内衣穿衬衫，穿了衬衫穿外套。

Data是事务层上层（诸如命令层、NVMe层）给的数据，事务层给它头上加个Header，然后尾巴上再加个CRC校验，就构成了一个TLP。这个TLP下传到数据链路层，又被数据链路层在头上加了个包序列号（Sequence Number，SN），尾巴上再加个CRC校验，然后下传到物理层。物理层为其头上加个Start，尾巴上加个End符号，把这些数据分派到各个Lane上，然后在每个Lane上加扰码，经8/10或128/130编码，最后通过物理传输介质传输给接收方，如图5-13所示。

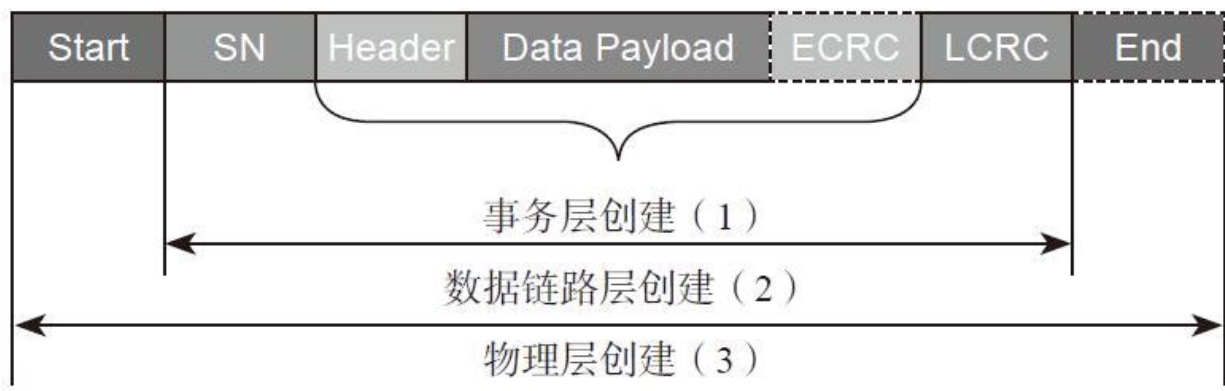


图5-13 发送方打包TLP过程

接收方物理层是最先接收到这些数据的，掐头（Start）去尾（End），然后交由上层。在数据链路层，校验序列号和LCRC，如果没问题，剥掉序列号和LCRC，往事务层走；如果校验出差，通知对方重传。在事务层，校验ECRC，有错，数据抛弃；没错，去掉ECRC，获得数据。整个过程犹如脱衣睡觉，外套脱了，衬衫脱了，内衣也脱了，光溜溜钻进被窝，如图5-14所示。

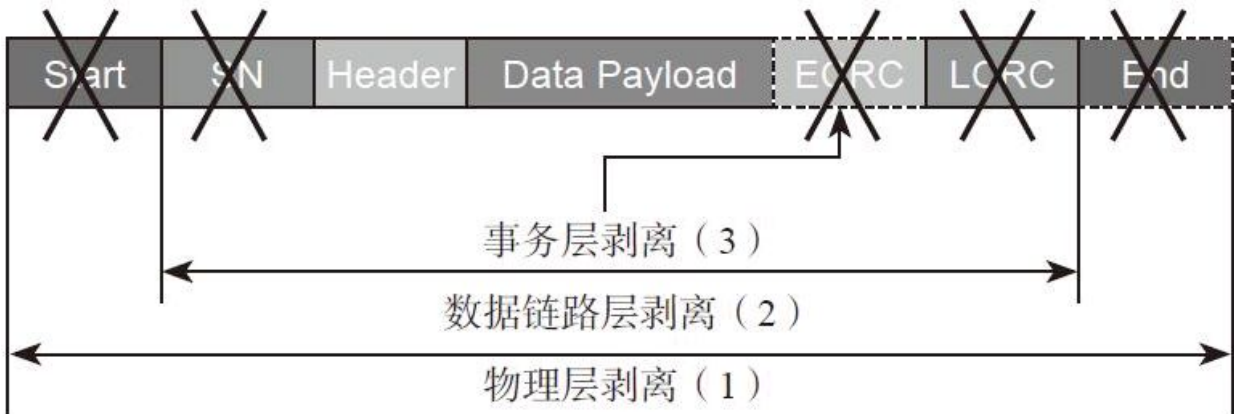


图5-14 接收方解包TLP过程

和PCI数据裸奔不同，PCIe的数据是穿衣服的。PCIe数据以Packet的形式传输，比起PCI冷冰冰的数据，PCIe的数据是鲜活有生命的。

每个Endpoint都需要实现这三层，每个Switch的Port也需要实现这三层（见图5-15）。

如图5-15所示，如果RC要与EP1通信，中间要经历怎样的一个过程？

如果把前述的数据发送和接收过程叫作穿衣和脱衣，那么，RC与EP1数据传输过程中，则存在好几次这样穿衣脱衣的过程：RC帮数据穿好衣服，发送给Switch的上游端口，A为了知道该笔数据发送给谁，就需要脱掉该数据的衣服，找到里面的地址信息。衣服脱光后，Switch发现它是往EP1的，又帮它换了身新衣服，发送给端口B。B又不嫌麻烦的脱掉它的衣服，换上新衣服，最后发送给EP1，如图5-16所示。

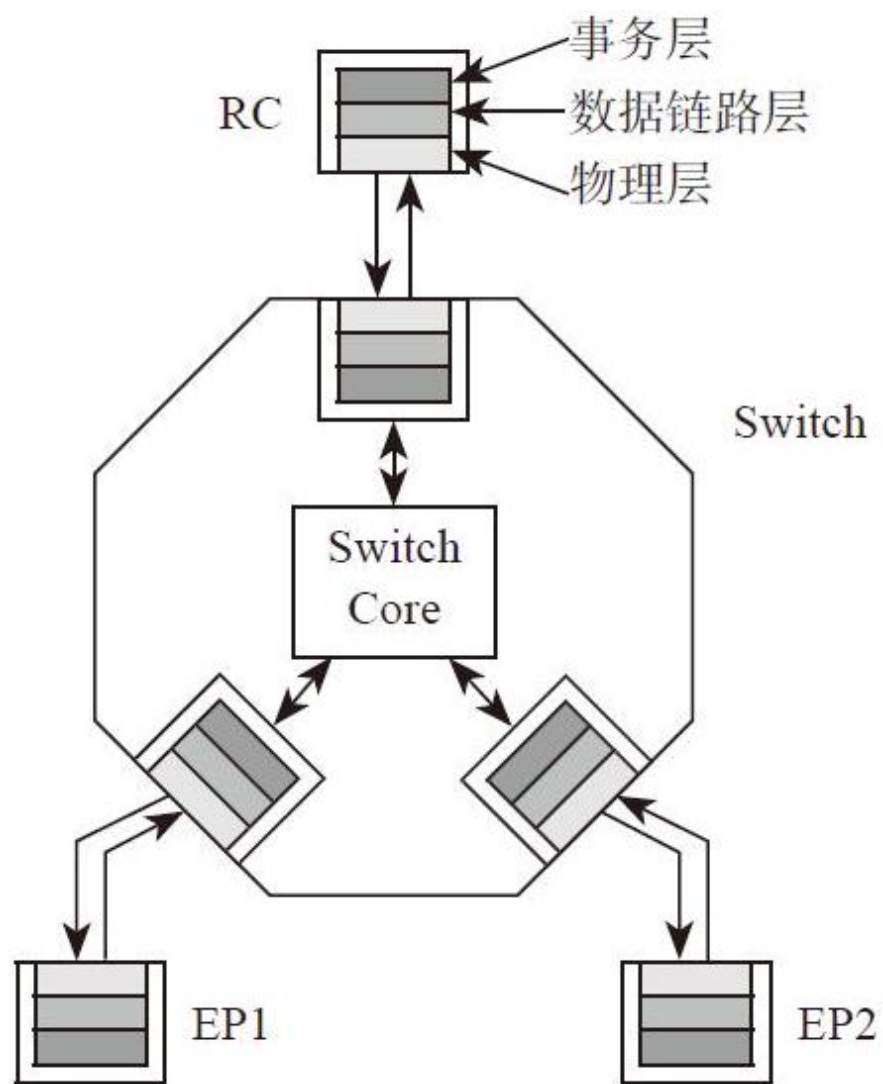


图5-15 RC、Switch和EP都要实现三层

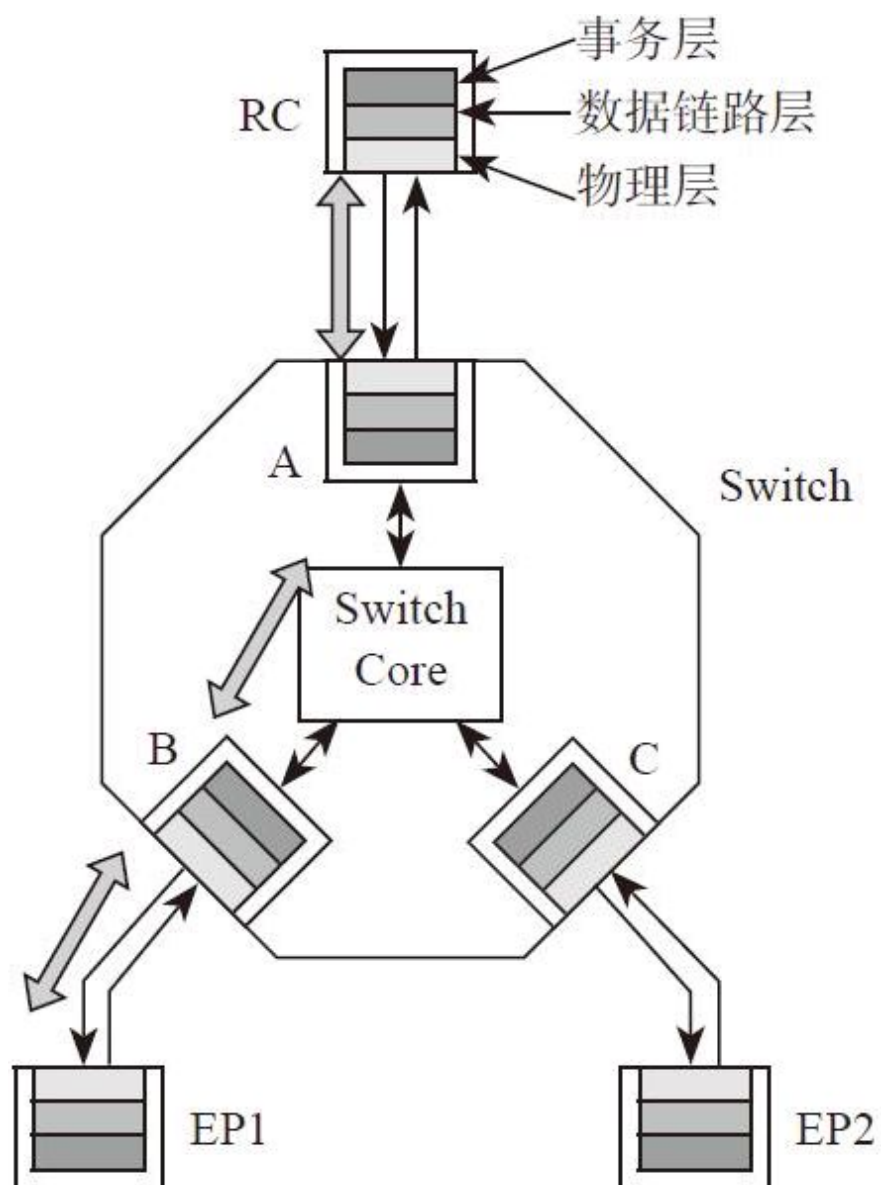


图5-16 RC和EP通信

Switch的主要功能是转发数据，为什么还需要实现事务层？Switch必须实现这三层，因为数据的目的地址信息是在TLP中的，如果不实现这一层，就无法知道目的地址，也就无法实现数据寻址路由。

5.4 PCIe TLP类型

主机与PCIe设备之间，或者PCIe设备与设备之间，数据传输都是以Packet形式进行的。事务层根据上层（软件层或者应用层）请求（Request）的类型、目的地址和其他相关属性，把这些请求打包，产生TLP（Transaction Layer Packet，事务层数据包）。然后这些TLP往下，经历数据链路层、物理层，最终到达目标设备。

根据软件层的不同请求，事务层产生四种不同的TLP请求：

- Memory;
- IO;
- Configuration;
- Message。

前三种分别用于访问内存空间、IO空间、配置空间，这三种请求在PCI或者PCI-X时代就有了，最后的Message请求是PCIe新加的。在PCI或者PCI-X时代，像中断、错误以及电源管理相关信息，都是通过边带信号（Sideband Signal）进行传输的，但PCIe干掉了这些边带信号线，所有的通信都是走带内信号，即通过Packet传输，因此，过去一些由边带信号线传输的数据，比如中断信息、错误信息等，现在就交由Message来传输了。

我们知道，一个设备的物理空间，可以通过内存映射（Memory Map）的方式映射到主机的主存，有些空间还可以映射到主机的IO空间（如果主机存在IO空间的话）。但新的PCIe设备（区别于Legacy PCIe设备）只支持内存映射，之所以还存在访问IO空间的TLP，完全是为了照顾那些老设备。以后IO映射的方式会逐渐取消，为减轻学习压力，我们以后看到IO相关的东西，大可忽略掉。

所有配置空间（Configuration）的访问，都是主机发起的，确切地说是RC发起的，往往只在上电枚举和配置阶段会发起配置空间的访问，这样的TLP很重要，但不是常态；Message也是一样，只有在有中断或者有错误等情况下，才会有Message TLP，这是非主流的。PCIe线

上主流传输的是Memory访问相关的TLP，主机与设备或者设备与设备之间，数据都是在彼此的Memory之间（抛掉IO）交互，因此，这种TLP是我们最常见的。

这四种请求，如果需要对方响应的，我们称之为Non-Posted TLP；如果不指望对方给响应的，我们称之为Posted TLP。Post，有“邮政”的意思，我们只管把信投到邮箱，能不能到达对方，就取决于邮递员了。Posted TLP，就是不指望对方回复（信能不能收到都是个问题）；Non-Posted TLP，就是要求对方务必回复。

哪些TLP是Posted，哪些又是Non-Posted的呢？像Configuration和IO访问，无论读写，都是Non-Posted的，这样的请求必须得到设备的响应；Message TLP是Posted的；Memory Read必须是Non-Posted的，我读你数据，你不返回数据（返回数据也是响应），那肯定不行，所以Memory Read必须得到响应；而Memory Write是Posted的，我数据传给你，无须回复，这样主机或者设备可以不等对方回复，趁早把下一笔数据写下去，这样一定程度上提高了写的性能。有人会担心如果没有得到对方的响应，发送者就没有办法知道数据究竟有没有成功写入，就有丢数据的风险。虽然这个风险存在（概率很小），但数据链路层提供了ACK/NAK机制，一定程度上能保证TLP正确交互，因此能很大程度上减小了数据写失败的可能。TLP的请求类型如表5-2所示。

表5-2 TLP请求类型

请求类型	Non-Posted / Posted
Memory Read	Non-Posted
Memory Write	Posted
Memory Read Lock	Non-Posted
IO Read	Non-Posted
IO Write	Non-Posted
Configuration Read (Type 0 和 Type 1)	Non-Posted
Configuration Write (Type 0 和 Type 1)	Non-Posted
Message	Posted

所以，只要记住只有Memory Write和Message两种TLP是Posted的就可以了，其他都是Non-Posted的。

Memory Read Lock是历史的遗留物，Native PCIe设备已经抛弃了它，它存在的意义完全是为了兼容Legacy PCIe设备。和IO一样，我们

也可以忽略。能不看的就不看，PCIe内容本来就多，不要被这些过时没用的东西挡住我们学习的道路。

在Configuration一栏，我们看到Type 0和Type 1。在之前的拓扑结构中，我们看到除了Endpoint之外，还有Switch，他们都是PCIe设备，但配置种类不同，因此用Type 0和Type 1区分，如表5-3所示。

表5-3 Native PCIe TLP类型

请求类型	Non-Posted / Posted
Memory Read	Non-Posted
Memory Write	Posted
Configuration Read (Type 0 和 Type 1)	Non-Posted
Configuration Write (Type 0 和 Type 1)	Non-Posted
Message	Posted

这样，Request TLP是不是清爽点？

对Non-Posted的Request，是一定需要对方响应的，对方需要通过返回一个Completion TLP来作为响应。对Read Request来说，响应者通过Completion TLP返回请求者所需的数据，这种Completion TLP包含有效数据；对Write Request（现在只有Configuration Write了）来说，响应者通过Completion TLP告诉请求者执行状态，这样的Completion TLP不含有效数据。

因此，PCIe里面所有的TLP=Request TLP+Completion TLP。

表5-4 Native PCIe请求和响应TLP类型

TLP 数据包类型	缩写
Memory Read	MRd
Memory Write	MWr
Configuration Read (Type 0 和 Type 1)	CfgRd0, CfgRd1
Configuration Write (Type 0 和 Type 1)	CfgWr0, CfgWr1
Message Request with Data	MsgD
Message Request without Data	Msg
Completion with Data	CplD
Completion without Data	Cpl

看个Memory Read的例子，如图5-17所示。

例子中，PCIe设备C想读主机内存的数据，因此，它在事务层上生成一个Memory Read TLP，该MRd一路向上，到达RC。RC收到该Request，就到内存中取PCIe设备C所需的数据，RC通过Completion with Data TLP（CplD）返回数据，原路返回，直到PCIe设备C。

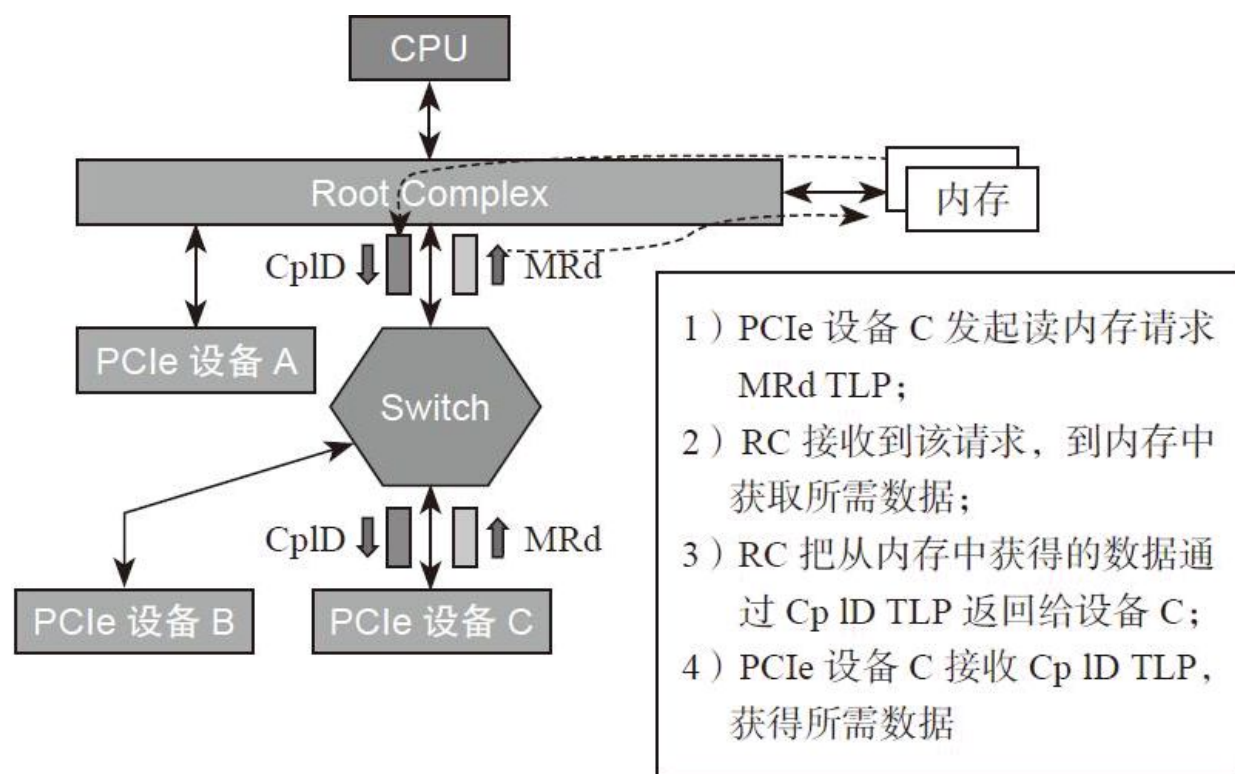


图5-17 MemoryRead示例

一个TLP最多只能携带4KB有效数据，因此，上例中，如果PCIe设备C需要读16KB的数据，则RC必须返回4个CplD给PCIe设备C。注意，PCIe设备C只需发1个MRd就可以了。

再看个Memory Write的例子，如图5-18所示。

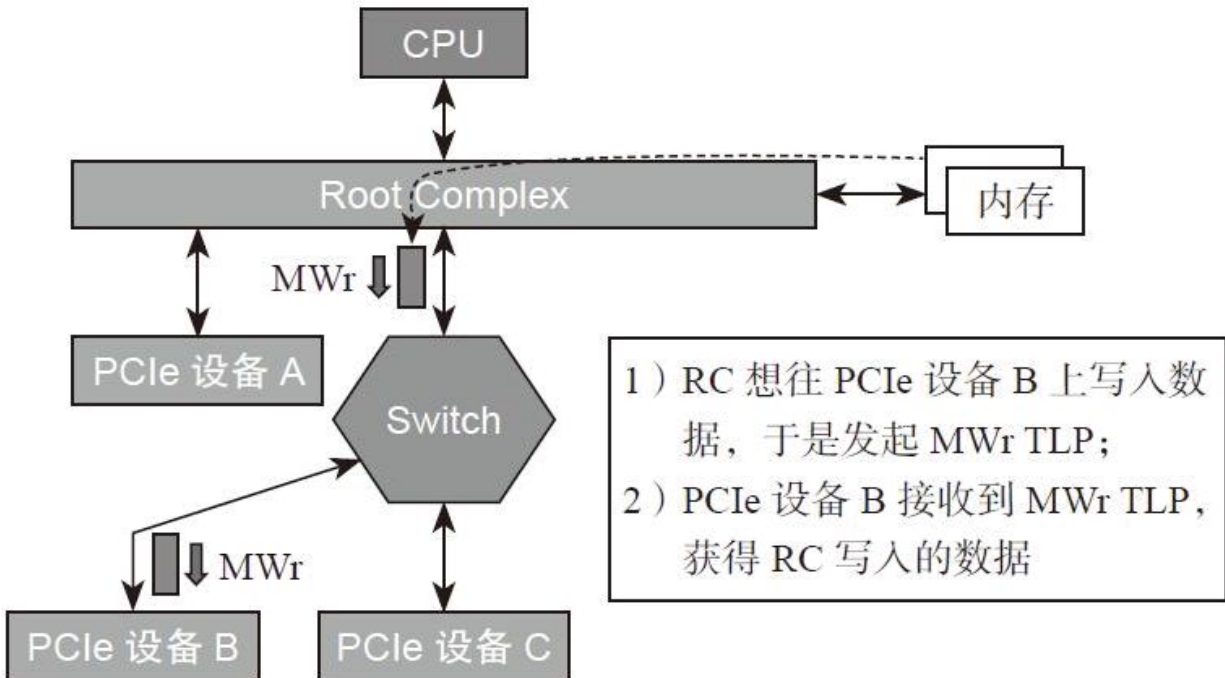


图5-18 MemoryWrite示例

该例中，主机想往PCIe设备B中写入数据，因此RC在其事务层生成了一个Memory Write TLP（要写的数据在该TLP中），通过Switch直到目的地。前面说过Memory Write TLP是Posted的，因此，PCIe设备B收到数据后，不需要返回Completion TLP（如果这时返回Completion TLP，反而是画蛇添足）。

同样的，由于一个TLP只能携带4KB数据，因此主机想往PCIe设备B上写入16KB数据，RC必须发送4个MW_r TLP。

5.5 PCIe TLP结构

无论Request TLP，还是作为回应的Completion TLP，它们的模样都差不多，如图5-19所示。

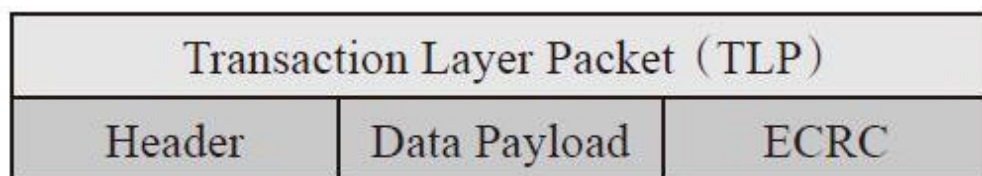


图5-19 TLP数据格式

TLP主要由三部分组成：Header、Data（可选，取决于具体TLP类型）和ECRC（可选）。TLP都是始于发送端的事务层（Transaction Layer），终于接收端的事务层。

每个TLP都有一个Header，跟动物一样，没有头就活不了，所以TLP可以没手没脚，但不能没有头。事务层根据上层请求内容，生成TLP Header。Header内容包括发送者的相关信息、目标地址（该TLP要发给谁）、TLP类型（诸如前面提到的Memory Read、Memory Write）、数据长度（如果有的话）等。

Data Payload域，用以放有效载荷数据。该域不是必需的，因为并不是每个TLP都必须携带数据，比如Memory Read TLP，它只是一个请求，数据是由目标设备通过Completion TLP返回的。后面我们会整理哪些TLP需要携带数据，哪些TLP不带数据。前面也提到，一个TLP最大载重是4KB，数据长度大于4KB的话，就需要分几个TLP传输。

ECRC（End to End CRC）域，它对之前的Header和Data（如果有的话）生成一个CRC，在接收端根据收到的TLP重新生成Header和Data（如果有的话）的CRC，与收到的CRC比较，一样则说明数据在传输过程中没有出错，否则就有错。它也是可选的，可以设置不加CRC。

Data域和CRC域没有什么好说的，有花头的是Header域，我们要深入其中看看。

一个Header大小可以是3DW，也可以是4DW。以4DW的Header为例，TLP的Header如下所示（见图5-20）。

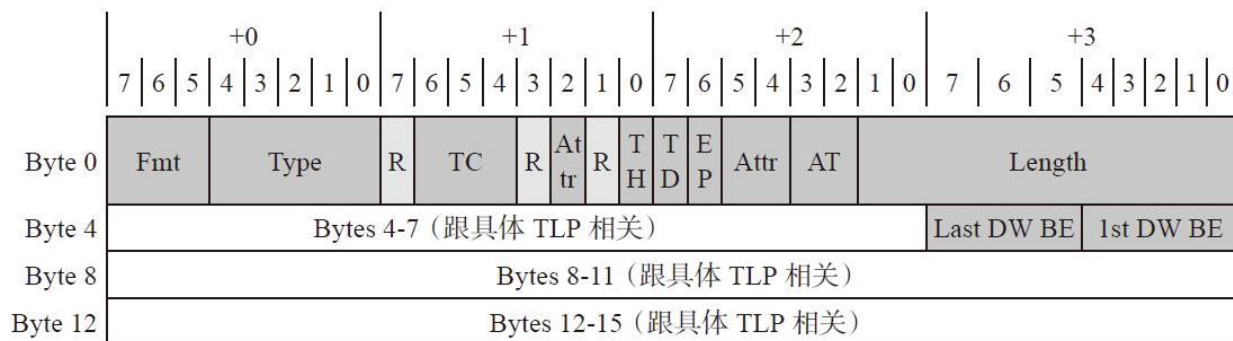


图5-20 TLP的Header格式

深色区域为所有TLP Header公共部分，所有Header都有这些；其他则跟具体的TLP相关。

稍微解释一下：

·Fmt: Format，表明该TLP是否带有数据，Header是3DW还是4DW。

·Type: TLP类型，上一节提到的，包括Memory Read、Memory Write、Configuration Read、Configuration Write、Message和Completion等。

·R: Reserved，等于0。

·TC: Traffic Class，TLP也分三六九等，优先级高的先得到服务。TC: 3bit，说明可以分为8个等级，0~7，TC默认是0，数字越大，优先级越高。

·Attr: Attribute，属性，前后共三个bit。

·TH: TLP Processing Hints。

·TD: TLP Digest，之前说ECRC可选，如果这个bit置起来，说明该TLP包含ECRC，接收端应该做CRC校验。

·EP: Poisoned Data，“有毒”的数据，远离。

·AT: Address Type, 地址种类。

·Length: Payload数据长度, 10个bit, 最大为1024, 单位为DW, 所以TLP最大数据长度是4KB; 该长度总是DW的整数倍, 如果TLP的数据不是DW的整数倍 (不是4Byte的整数倍), 则需要用到Last DW BE和1st DW BE这两个域。

到目前为止, 对于Header, 我们只需知道它大概有什么内容, 没有必要记住每个域是什么。

这里重点讲讲Fmt和Type, 看看不同TLP (这里所列为精简版的, 仅为Native PCIe设备所支持的TLP) 的Fmt和Type应该怎样编码 (见表5-5)。

表5-5 TLP格式和类型域编码

TLP	Fmt 域	Type 域	说明
Memory Read Request	000=3DW, 不带数据 001=4DW, 不带数据	0 0000	Memory Read 不带数据, 其 Header 大小为 3DW 或 4DW
Memory Write Request	010=3DW, 带数据 011=4DW, 带数据	0 0000	Memory Write 带数据, 其 Header 大小为 3DW 或 4DW
Configuration Type 0 Read Request	000=3DW, 不带数据	0 0100	读 Endpoint 的 Configuration, 不带数据, Header 总是 3DW
Configuration Type 0 Write Request	010=3DW, 带数据	0 0100	写 Endpoint 的 Configuration, 带数据, Header 总是 3DW
Configuration Type 1 Read Request	000=3DW, 不带数据	0 0101	读 Switch 的 Configuration, 不带数据, Header 总是 3DW
Configuration Type 1 Write Request	010=3DW, 带数据	0 0101	写 Switch 的 Configuration, 带数据, Header 总是 3DW
Message Request	001=4DW, 不带数据	1 0rrr	Message 的 Header 总是 4DW
Message Request with Data	011 = 4DW, 带数据	1 0rrr	Message 的 Header 总是 4DW
Completion	000=3DW, 不带数据	0 1010	Completion 的 Header 总是 3DW
Completion with Data	010=3DW, 带数据	0 1010	Completion 的 Header 总是 3DW

如表5-5所示, Configuration和Completion的TLP (以C打头的TLP) 的Header大小总是3字节; Message TLP的Header总是4字节。而Memory相关TLP的Header取决于地址空间的大小, 地址空间小于4GB的, Header大小为3DW; 大于4GB的, Header大小则为4DW。

上面介绍了几个TLP Header的通用部分, 下面分别介绍具体TLP的Header。

1.Memory TLP

有两个重要的内容在前面没有提到，那就是TLP的源和目标。即该TLP是哪里产生的，它要到哪里去，这些信息都是包含在Header里面的。因为不同的TLP类型，寻址方式不同，因此要结合具体TLP来看。

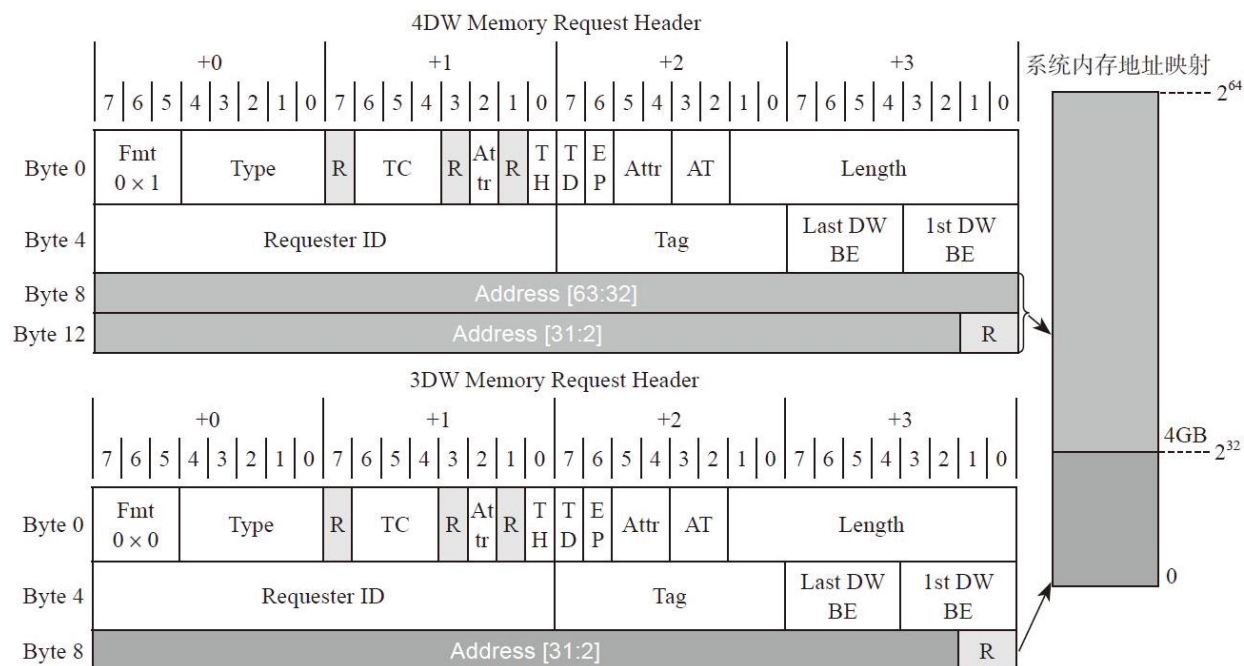


图5-21 Memory TLP的Header

对一个PCIe设备来说，它开放给主机访问的设备空间首先会映射到主机的内存空间，主机如果想访问设备的某个空间，TLP Header当中的地址应该设置为该访问空间在主机内存的映射地址。如果主机内存空间小于4GB，则Memory读写TLP的Header大小为3DW；大于4GB，则为4DW。对4GB内存空间，32bit的地址用1DW就可以表示，该地址位于Byte8-11；而4GB以上的内存空间，需要用2DW表示地址，该地址位于Byte8-15。

该TLP经过Switch的时候，Switch会根据地址信息，把该TLP转发到目标设备。之所以能唯一地找到目标设备，是因为不同的Endpoint设备空间会映射到主机内存空间的不同位置。

关于TLP路由，后文还会详细介绍。

Memory TLP的目标是通过内存地址告知的，而源则是通过“Requester ID”告知的。每个设备在PCIe系统中都有唯一的ID，该ID由总线（Bus）、设备（Device）、功能（Function）三者唯一确定。这个后面也会专门讲，这里只需知道一个PCIe组成有唯一的一个ID，不管是RC、Switch还是Endpoint。

2.Configuration TLP

Endpoint和Switch的配置（Configuration）格式不一样，分别由Type 0和Type 1来表示。配置可以认为是一个Endpoint或者Switch的标准空间，这段空间在初始化时需要映射到主机的内存空间。与设备的其他空间不同，该空间是标准化的，即不管是哪个厂家生产的设备，都需要有这段空间，而且哪个地方放什么东西，都是协议规定好的，主机按协议访问这部分空间。主机软件访问PCIe设备的配置空间，RC会生成Configuration TLP与Switch或EP交互。

如表5-22所示是访问Endpoint的配置空间的TLP Header（Type 0）。

	+0								+1								+2								+3													
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0						
Byte 0	Fmt 0 × 0			Type 0010 ×					R	TC 000				R	At tr 0	R	TH 0	T D	E P	Attr 00		AT 00	Length 0000000001															
Byte 4	Requester ID																Tag						Last DW BE 0000				1st DW BE											
Byte 8	Bus Number								Device				Func				Rsvd				Ext Reg Number				Register Number								R					
									Function Number with ARI																													

图5-22 Type 0 Configuration TLP的Header

Bus Number+Device+Function就唯一决定了目标设备；Ext Reg Number+Register Number相当于配置空间的偏移。找到了设备，然后指定了配置空间的偏移，就能找到具体想访问的配置空间的某个位置（寄存器）。

3.Message TLP

Message TLP用于传输中断、错误、电源管理等信息，取代PCI时代的边带信号传输。Message TLP的Header大小总是4DW，如图5-23所示。

Message Code指定该Message的类型，具体如下图5-24所示。

不同的Message Code，最后两个DW的意义也不同，这里不再展开。

4.Completion TLP

有Non-Posted Request TLP，才有Completion TLP，有因才有果。前面看到，Requester的TLP当中都有Requester ID和Tag，来告知接收者、发起者是谁。那么响应者的目标地址很简单，照抄发起者的源地址就可以了。Completion TLP的Header如图5-25所示。

	+0								+1								+2								+3							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Byte 0	Fmt 0 × 1		Type 10rrr						R	TC		R	Attr	R	TH 0	T D	E P	Attr 00	AT 00	Length												
Byte 4	Requester ID																Tag						Message Code									
Byte 8	Bytes 8-11 (跟 Message code 相关)																															
Byte 12	Bytes 12-15 (跟 Message code 相关)																															

图5-23 Message TLP的Header

Message Code [7:0]	Byte 7 Bit 7:0	这个域表示发送message的类型
		0000 0000b = Unlock Message
		0001 0000b = Lat. Tolerance Reporting
		0001 0010b = Optimized Buffer Flush/Fill
		0001 xxxxb = Power Mgt. Message
		0010 0xxxb = INTx Message
		0011 00xxb = Error Message
		0100 xxxxb = Ignored Messages
		0101 0000b = Set Slot Power Message
		0111 111xb = Vendor-Defined Messages

图5-24 Messagecode域解释

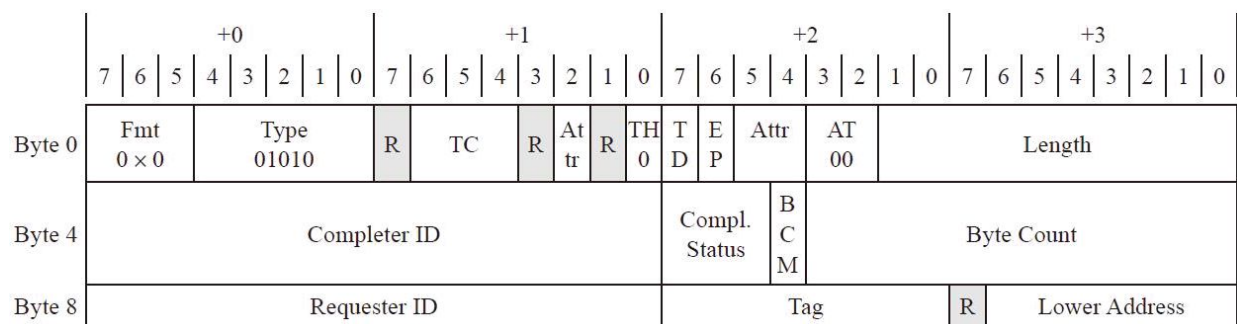


图5-25 Completion TLP的Header

Completion TLP一方面，可以返回请求者的数据，比如作为Memory或Configuration Read的响应；另一方面，还可以返回该事务（Transaction）的状态。因此，在Completion TLP的Header中有一个Completion Status，用以返回事务状态（见图5-26）。

域名称	Header Byte/Bit	解释
Compl. Status [2:0] (Completion Status Code)	Byte 6 Bit 7:5	These bits indicate status for this Completion. 000b = Successful Completion (SC) 001b = Unsupported Request (UR) 010b = Config Req Retry Status (CRS) 100b = Completer abort (CA)

图5-26 Completion Status Code

5.6 PCIe配置和地址空间

每个PCIe设备都有这样一段空间，主机软件可以通过读取它获得该设备的一些信息，也可以通过它来配置该设备，这段空间就称为PCIe的配置空间。不同于每个设备的其他空间，PCIe设备的配置空间是协议规定好的，哪个地方放什么内容，都是有定义的。PCI或者PCI-X时代就有配置空间的概念，具体如图5-27所示。

整个配置空间就是一系列寄存器的集合，由两部分组成：64B的Header和192B的Capability数据结构。

进入PCIe时代，PCIe能耐更大，192B不足以罗列它的绝活。为了保持后向兼容，又要不把绝活落下，怎么办？很简单，扩展后者的空间，把整个配置空间由256B扩展成4KB，前面256B保持不变（见图5-28）。

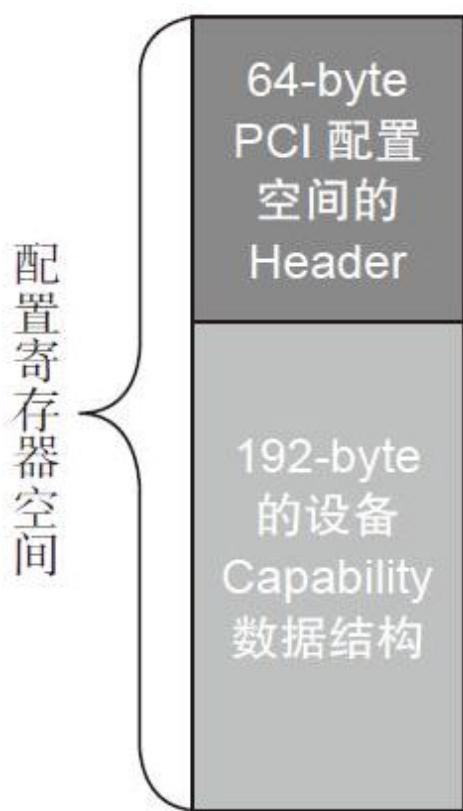


图5-27 PCI设备的256B配置空间

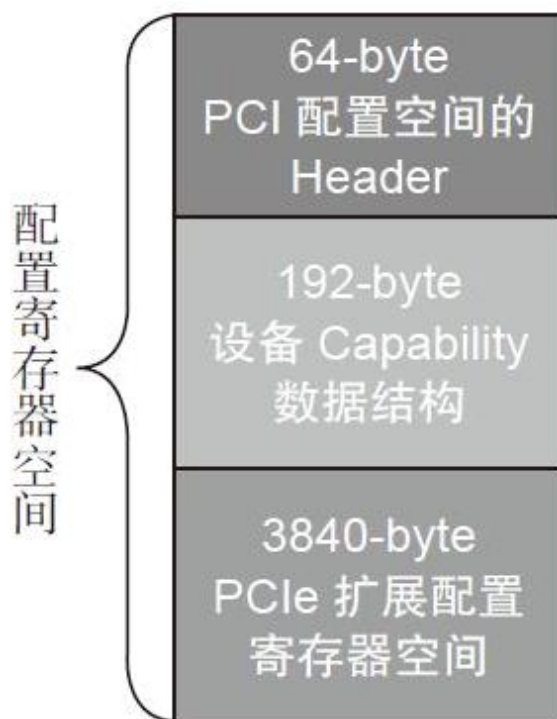


图5-28 PCIe设备的4KB配置空间

PCIe有什么能耐（Capability）我们不看，先看看只占64B的 Configuration Header（见图5-29）。

其中，Type 0 Header是Endpoint的Configuration Header，Type 1 Header是Switch的Configuration Header。

像Device ID、Vendor ID、Class Code和Revision ID是只读寄存器，PCIe设备通过这些寄存器告诉主机软件，这是哪个厂家的设备、设备ID是多少以及是什么类型的（网卡、显卡、桥）设备。

其他的我们暂时不看，我们看看重要的BAR（Base Address Register）。

对Endpoint Configuration（Type 0）提供了最多6个BAR，而对Switch（Type 1）来说只有2个。BAR是做什么的？

每个PCIe设备，都有自己的内部空间，这部分空间如果开放给主机（软件或者CPU）访问，那么主机怎样才能往这部分空间写入或者读数据呢？

我们知道，CPU只能直接访问主机内存（Memory）空间（或者IO空间），不能对PCIe等外设进行直接操作。怎么办？记得前文提到的RC吗？它可以为CPU分忧。

Type 0 Header				Doubleword	Type 1 Header				Doubleword
3	2	1	0		3	2	1	0	
Device ID		Vendor ID		00	Device ID		Vendor ID		00
Status		Command		01	Status		Command		01
Class Code			Revision ID	02	Class Code			Revision ID	02
BIST	Header Type	Latency Timer	Cache Line Size	03	BIST	Header Type	Latency Timer	Cache Line Size	03
Base Address 0				04	Base Address 0				04
Base Address 1				05	Base Address 1				05
Base Address 2				06	Secondary Latency Timer	Subordinate Bus Number	Secondary Bus Number	Primary Bus Number	06
Base Address 3				07	Secondary Status		I/O Limit	I/O Base	07
Base Address 4				08	Memory Limit		Memory Base		08
Base Address 5				09	Prefetchable Memory Limit		Prefetchable Memory Base		09
CardBus CIS Pointer				10	Prefetchable Base-Upper 32-bits				10
Subsystem ID		Subsystem Vendor ID		11	Prefetchable Limit-Upper 32-bits				11
Expansion ROM Base Address				12	I/O Limit Upper 16-bits		I/O Base Upper 16-bits		12
Reserved			Capabilities Pointer	13	Reserved		Capabilities Pointer		13
Reserved				14	Expansion ROM Base Address				14
Max_Lat	Min_Gnt	Interrupt Pin	Interrupt Line	15	Bridge Control		Interrupt Pin	Interrupt Line	15

图5-29 配置空间的Header

解决办法是：CPU如果想访问某个设备的空间，由于它不能亲自跟那些PCIe外设打交道，因此叫RC去办。比如，如果CPU想读PCIe外设的数据，先叫RC通过TLP把数据从PCIe外设读到主机内存，然后CPU从主机内存读数据；如果CPU要往外设写数据，则先把数据在内存中准备好，然后叫RC通过TLP写入到PCIe设备。

图5-30的最左边的虚线表示CPU要读Endpoint A的数据，RC则通过TLP（经历Switch）数据交互获得数据，并把它写入到系统内存中，然后CPU从内存中读取数据（深色实线箭头所示），从而CPU间接完成对PCIe设备数据的读取。

具体实现就是上电的时候，系统把PCIe设备开放的空间（系统软件可见）映射到内存地址空间，CPU要访问该PCIe设备空间，只需访问对应的内存地址空间。RC检查该内存地址，如果发现该内存空间地址是某个PCIe设备空间的映射，就会触发其产生TLP，去访问对应的PCIe设备，读取或者写入PCIe设备。

一个PCIe设备，可能有若干个内部空间（属性可能不一样，比如有些可预读，有些不可预读）需要映射到内存空间，设备出厂时，这些空间的大小和属性都写在Configuration BAR寄存器里面，上电后，系统软件读取这些BAR，分别为其分配对应的系统内存地址空间，并把相应的内存基地址写回到BAR（BAR的地址其实是PCI总线域的地址，CPU访问的是存储器域的地址，CPU访问PCIe设备时，需要把总线域地址转换成存储器域的地址）。

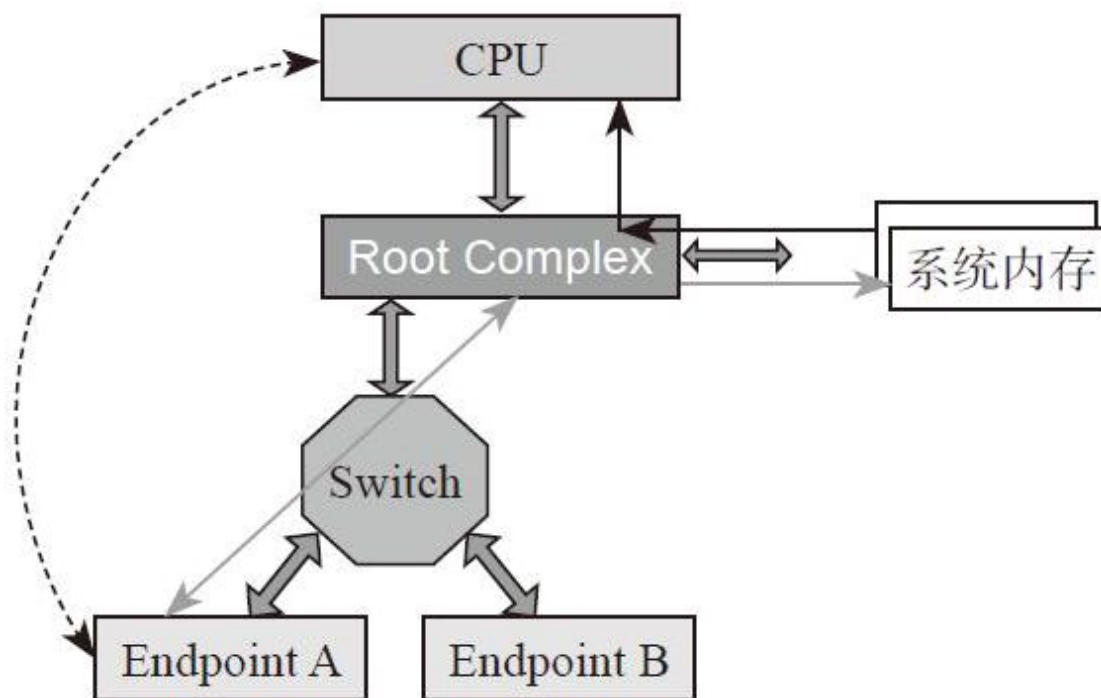


图5-30 CPU与EP通信示例

如图5-31所示，Native PCIe Endpoint（Switch右下）只支持Memory Map，它有两个不同属性的内部空间要开放给系统软件，因此，它可以分别映射到内存（Memory，不是DRAM区域）地址空间的两个地方；还有一个Legacy Endpoint，它既支持Memory Map，还支持IO Map，它也有两个不同属性的内部空间，分别映射到系统内存空间和IO空间。

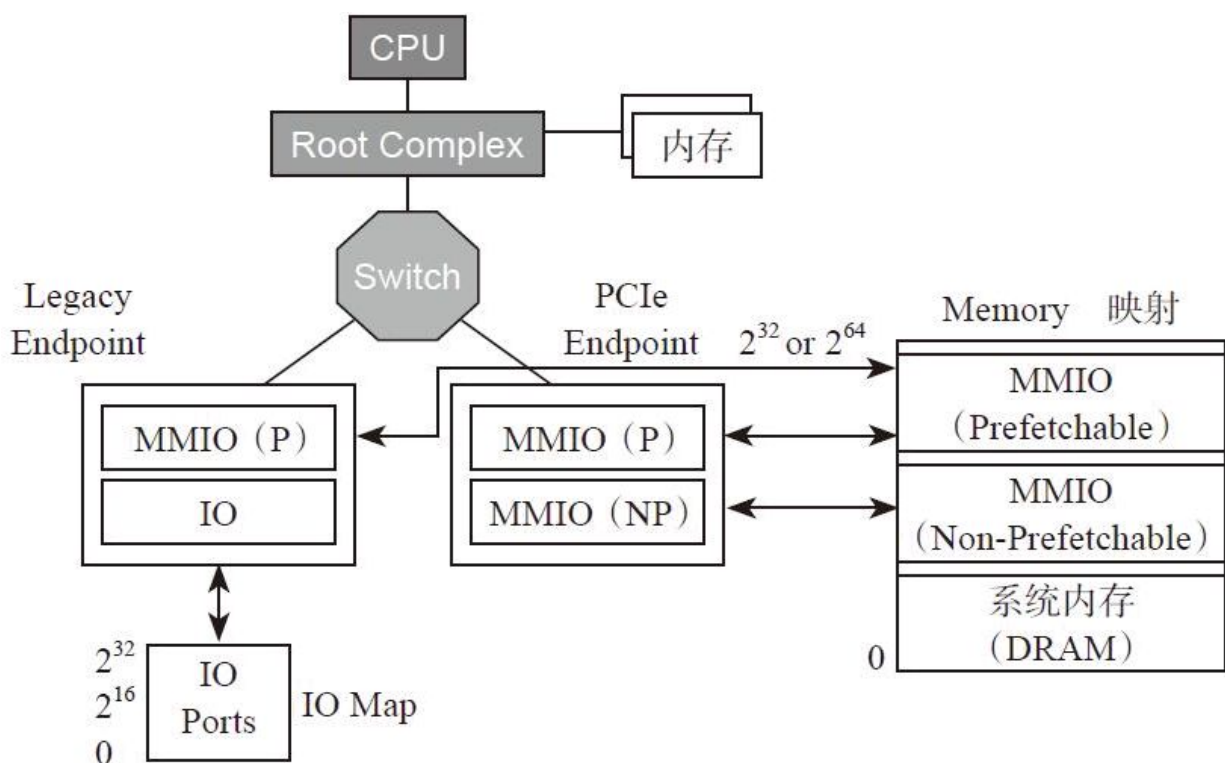


图5-31 Memory映射和I/O映射示例

下面，我们来看一下，对于PCIe设备，系统软件是如何为其分配映射空间的（见图5-32）。

上电时，系统软件首先会读取PCIe设备的BAR0，得到数据（见图5-33）

然后系统软件往该BAR0写入全1（见图5-34）。

BAR寄存器有些bit是只读的，是PCIe设备在出厂前就固定好的bit，写全1进去，如果值保持不变，就说明这些bit是厂家固化好的，这些固化好的bit提供了这块内部空间的一些信息：

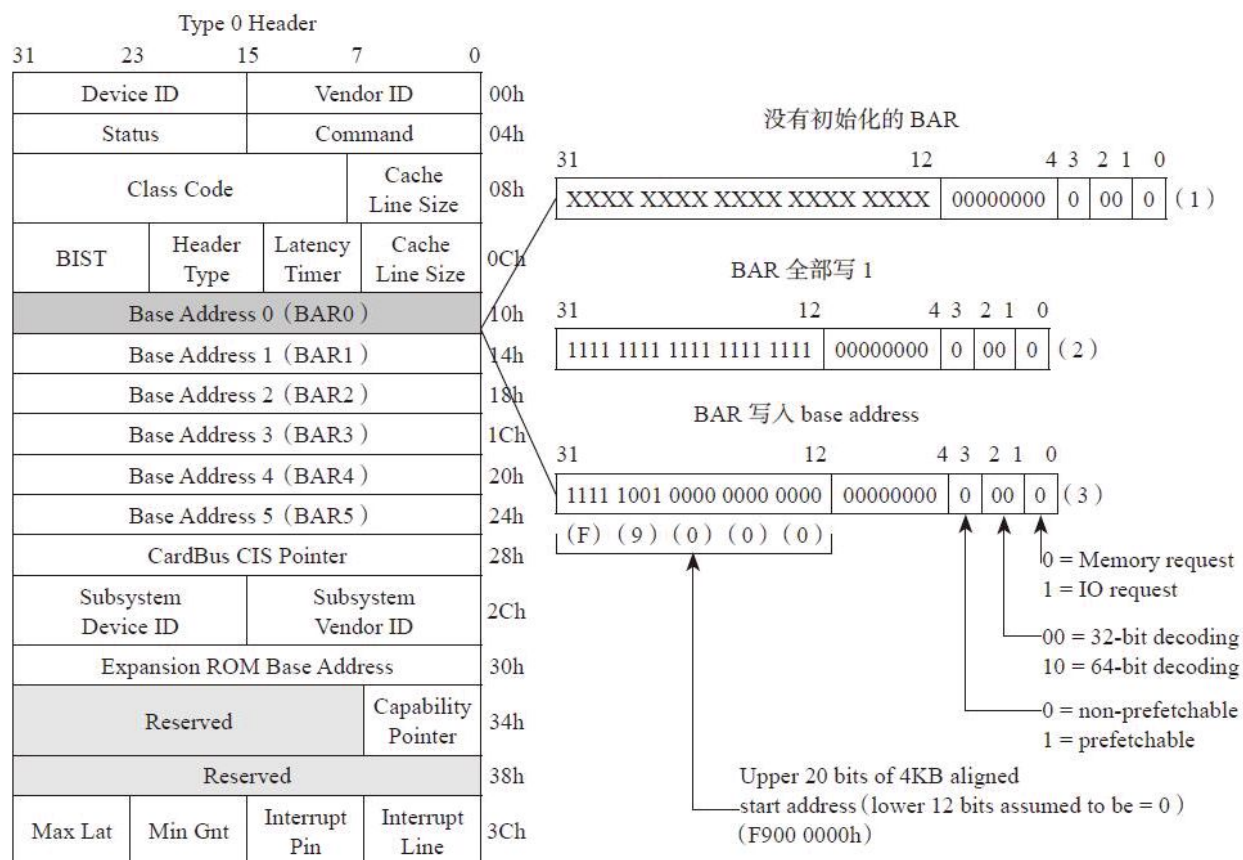


图5-32 BAR0设置示例

没有初始化的 BAR

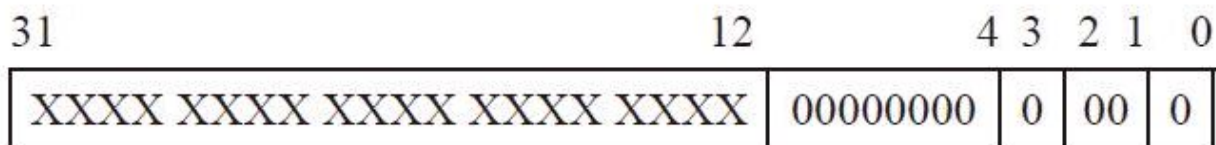


图5-33 设备初始BAR0值

BAR 全部写 1

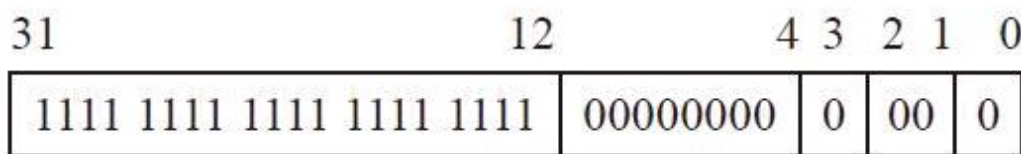


图5-34 系统软件往BAR0写入全1后的值

如何解读？低12位没变，表明该设备空间大小是4KB（2的12次方字节），然后低4位表明了该存储空间的一些属性（IO映射还是内存映射？32bit地址还是64bit地址？能否预取？做过单片机的人可能知道，有些寄存器只要一读，数据就会清掉，因此，对这样的空间，是不能预读的，因为预读会改变原来的值），这些都是PCIe设备在出厂前都设置好的，提供给系统软件的信息。

然后系统软件根据这些信息，在系统内存空间找到这样一块地方来映射这4KB的空间，把分配的基地址写入到BAR0（见图5-35）。

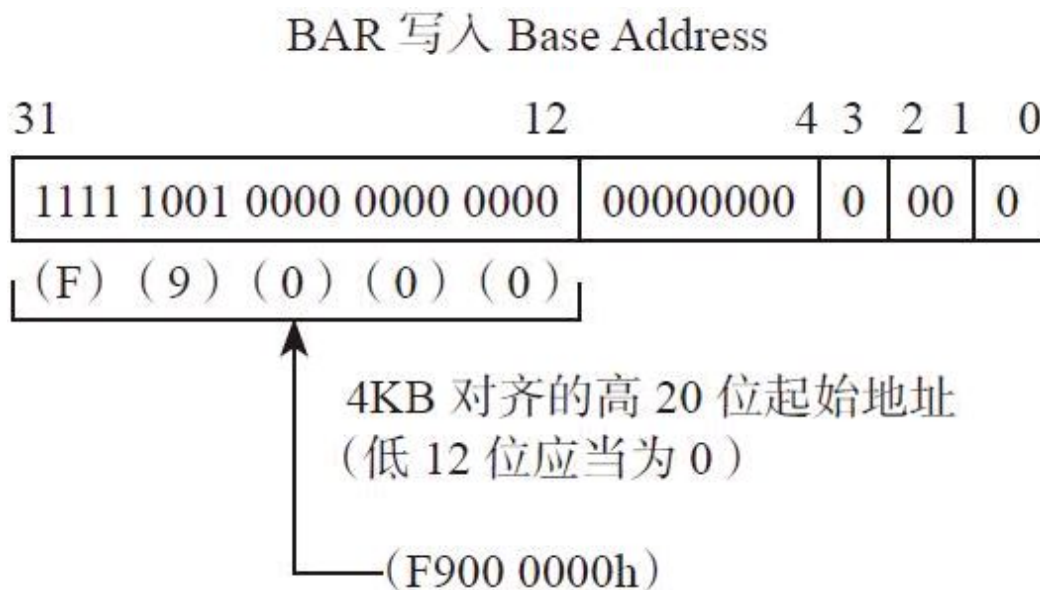


图5-35 主机软件为该空间分配地址空间后BAR0的值

从而完成了该PCIe空间的映射。一个PCIe设备可能有若干个内部空间需要开放出来，系统软件依次读取BAR1、BAR2……直到BAR5，完成所有内部空间的映射。

上面主要讲了Endpoint的BAR，Switch也有两个BAR，这里不展开讲，下节讲TLP路由的时候再回过头来讲。下面我们继续说配置空间。

前面说每个PCIe设备都有一个配置空间，其实这样的说法是不准确的，而是每个PCIe设备至少有一个配置空间。一个PCIe设备可能具有多个功能（Function），比如既能当硬盘，还能当网卡，每个功能对应一个配置空间。

寻址基本单元是功能，它的ID由Bus+Device+Function组成（BDF）。一个PCIe系统，可以最多有256条Bus，每条Bus上最多可以挂32个设备，而每个设备最多又能实现8个Function，每个Function对应4KB的配置空间。上电时，这些配置空间都需要映射到主机的内存地址空间（PCIe域，非DRAM区域）。这块内存地址映射区域大小为： $256 \times 32 \times 8 \times 4\text{KB} = 256\text{MB}$ 。注意，这只是内存空间的某个区域，不占用DRAM空间。

系统软件如何读取Configuration空间呢？不能通过BAR中的地址，为什么？别忘了BAR是在Configuration中的，你首先要读取Configuration，才能得到BAR。系统不是为所有可能的Configuration空间做了内存映射吗？系统软件想访问哪个Configuration，只需指定相应Function对应的内存空间地址，RC发现这个地址是Configuration映射空间，就会产生相应的Configuration Read TLP（映射地址→BDF）去获得相应Function的Configuration。

再回想一下前面介绍的Configuration Read TLP的Header格式（见图5-37）。

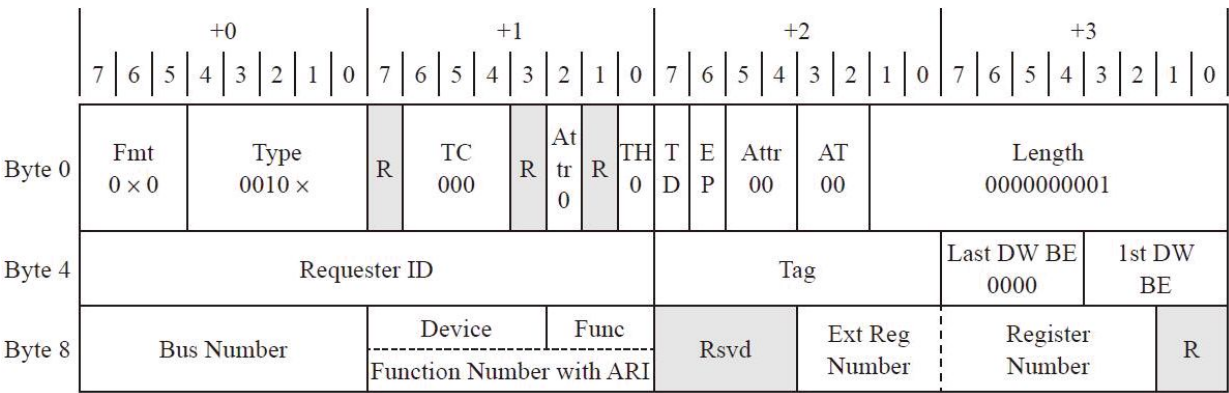


图5-37 ConfigurationRead TLP的Header

Bus Number+Device+Function就唯一决定了目标设备；Ext Reg Number+Register Number相当于配置空间的偏移。找到设备，然后指定配置空间的偏移，就能找到具体想访问的配置空间的某个位置（寄存器）。

请注意，只有RC才能发起Configuration的访问请求，其他设备是不允许对别的设备进行Configuration读写的。

5.7 TLP的路由

一个TLP是怎样历经千山万水，最后顺利抵达目的地的呢？

下面就以图5-38所示的简单拓扑结构为例，讨论一个TLP是怎样从发起者到达接收者，即TLP的路由问题。

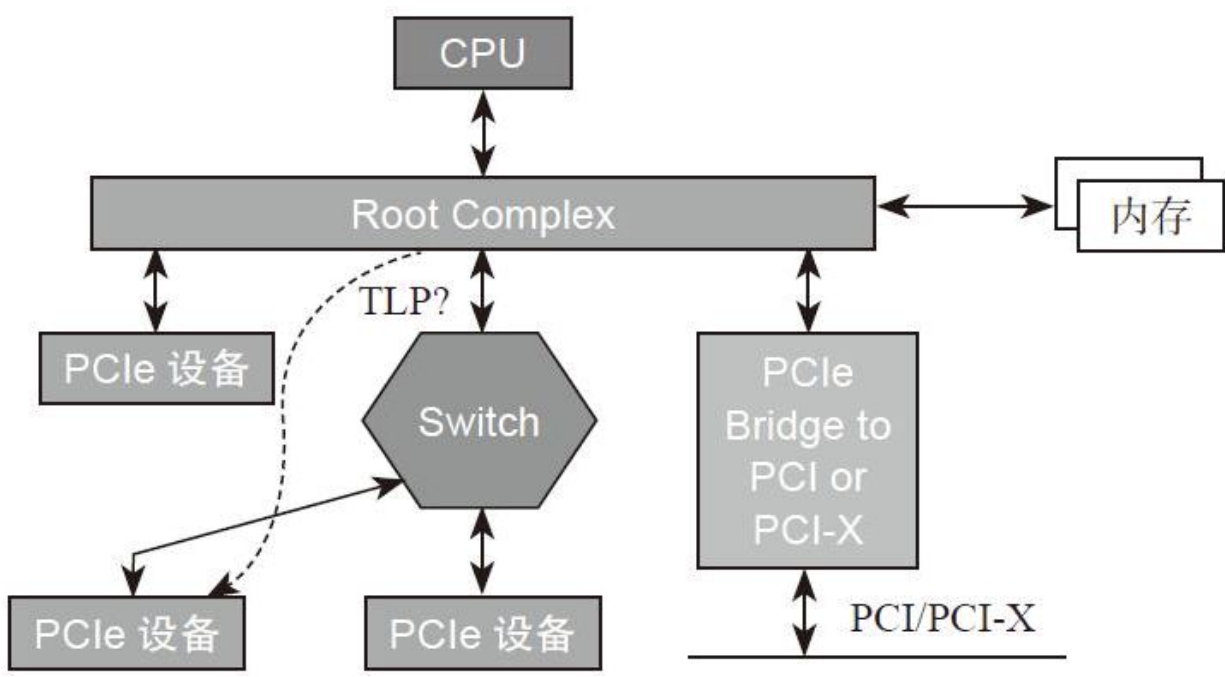


图5-38 TLP如何传输？

PCIe共有三种路由方式：基于地址（Memory Address）路由、基于设备ID（Bus Number+Device Number+Function Number）路由，还有就是隐式（Implicit）路由。

表5-6 TLP路由方式

TLP 类型	路由方式
Memory Read/Write TLP	地址路由
Configuration Read/Write TLP	ID 路由
Completion TLP	ID 路由
Message TLP	地址路由或者 ID 路由或者隐式路由

不同类型的TLP，其寻址方式也不同，表5-6总结了每种TLP对应的路由方式。

下面分别讲述这几种路由方式。

1.地址路由

前面提到，Switch负责路由和TLP的转发，而路由信息是存储在Switch的Configuration空间的，因此，很有必要先理解Switch的Configuration（见图5-39）。

BAR0和BAR1没有什么好说，跟前节讲的Endpoint的BAR意义一样，存放Switch内部空间在主机内存空间映射基址。

Switch有一个上游端口（靠近RC）和若干个下游端口，每个端口其实是一个Bridge，都有一个Configuration，每个Configuration描述了其下面连接设备空间映射的范围，分别由Memory Base和Memory Limit来表示。对上游端口，其Configuration描述的地址范围是它下游所有设备的映射空间范围，而对每个下游端口的Configuration，描述了连接它端口设备的映射空间范围。

前面我们看到，Memory Read或者Memory Write TLP的Header里面都有一个地址信息，该地址是PCIe设备内部空间在内存中的映射地址（见图5-40）。

当一个Endpoint收到一个Memory Read或者Memory Write TLP，它会把TLP Header中的地址跟Configuration当中所有的BAR寄存器比较，如果TLP Header中的地址落在这些BAR的地址空间，那么它就认为该TLP是发给它的，于是接收该TLP，否则就忽略，如图5-41所示。

Type 1 Header				
31		15		0
Device ID		Vendor ID		00h
Status		Command		04h
Class Code			Cache Line Size	08h
BIST	Header Type	Latency Timer	Cache Line Size	0Ch
Base Address 0 (BAR0)				10h
Base Address 1 (BAR1)				14h
Secondary Lat Timer	Subordinate Bus #	Secondary Bus #	Primary Bus #	18h
Secondary Status		IO Limit	IO Base	1Ch
Non-prefetchable Memory Limit		Non-prefetchable Memory Base		20h
Prefetchable Memory Limit		Prefetchable Memory Base		24h
Prefetchable Memory Base Upper 32 Bits				28h
Prefetchable Memory Limit Upper 32 Bits				2Ch
IO Limit Upper 16Bits		IO Base Upper 16 Bits		30h
Reserved			Capability Pointer	34h
Expansion ROM Base Address				38h
Bridge Control		Interrupt Pin	Interrupt Line	3Ch

图5-39 Type 1 Configuration Header

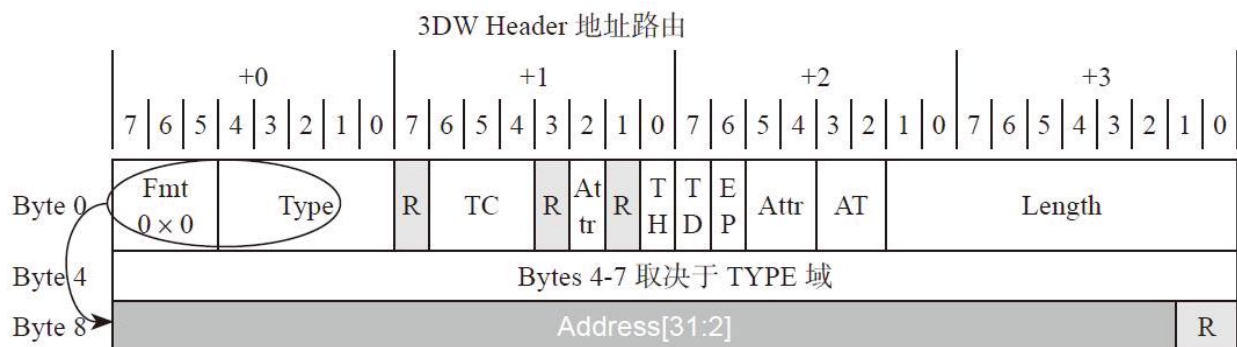


图5-40 地址路由3DW的TLP Header

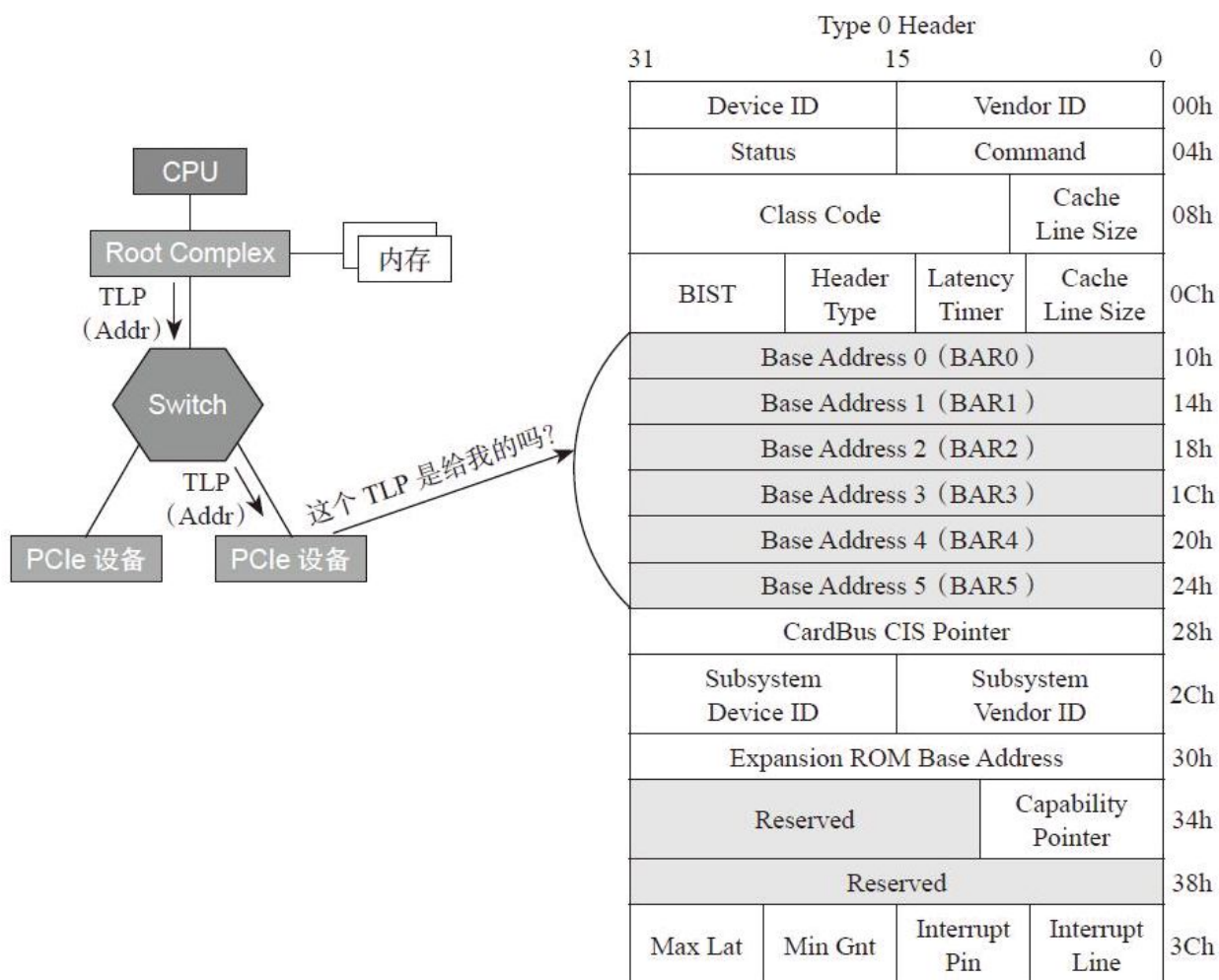


图5-41 EP通过对比目的地址和自己的BAR决定是否接收该TLP

当一个Switch上游端口收到一个Memory Read或者Memory Write TLP，它首先把TLP Header中的地址跟它自己Configuration当中的所有BAR寄存器比较，如果TLP Header当中的地址落在这些BAR的地址空间，那么它就认为该TLP是发给它的，于是接收该TLP（这个过程与

Endpoint的处理方式一样)；如果不是，则看这个地址是否落在其下游设备的地址范围内（是否在**Memory Base**和**Memory Limit**之间），如果是，说明该**TLP**是发给它下游设备的，因此它要完成路由转发；如果地址不落在下游设备的地方范围内，说明该**TLP**不是发给它下游设备的，则不接受该**TLP**，如图5-42所示。

刚才的描述是针对**TLP**从Upstream流到Downstream的路由。如果**TLP**从下游往上走呢？

它（某端口）首先把**TLP Header**中的地址跟它自己**Configuration**中的所有**BAR**寄存器比较，如果**TLP Header**当中的地址落在这些**BAR**的地址空间，那么它就认为该**TLP**是发给它的，于是接收该**TLP**（跟前面描述一样）；如果不是，那就看这个地址是否落在其下游设备的地址范围内（是否在**Memory Base**和**Memory Limit**之间）。如果是，这个时候不是接受，而是拒绝；相反，如果地址不落在下游设备的地址范围内，**Switch**则把该**TLP**传上去。

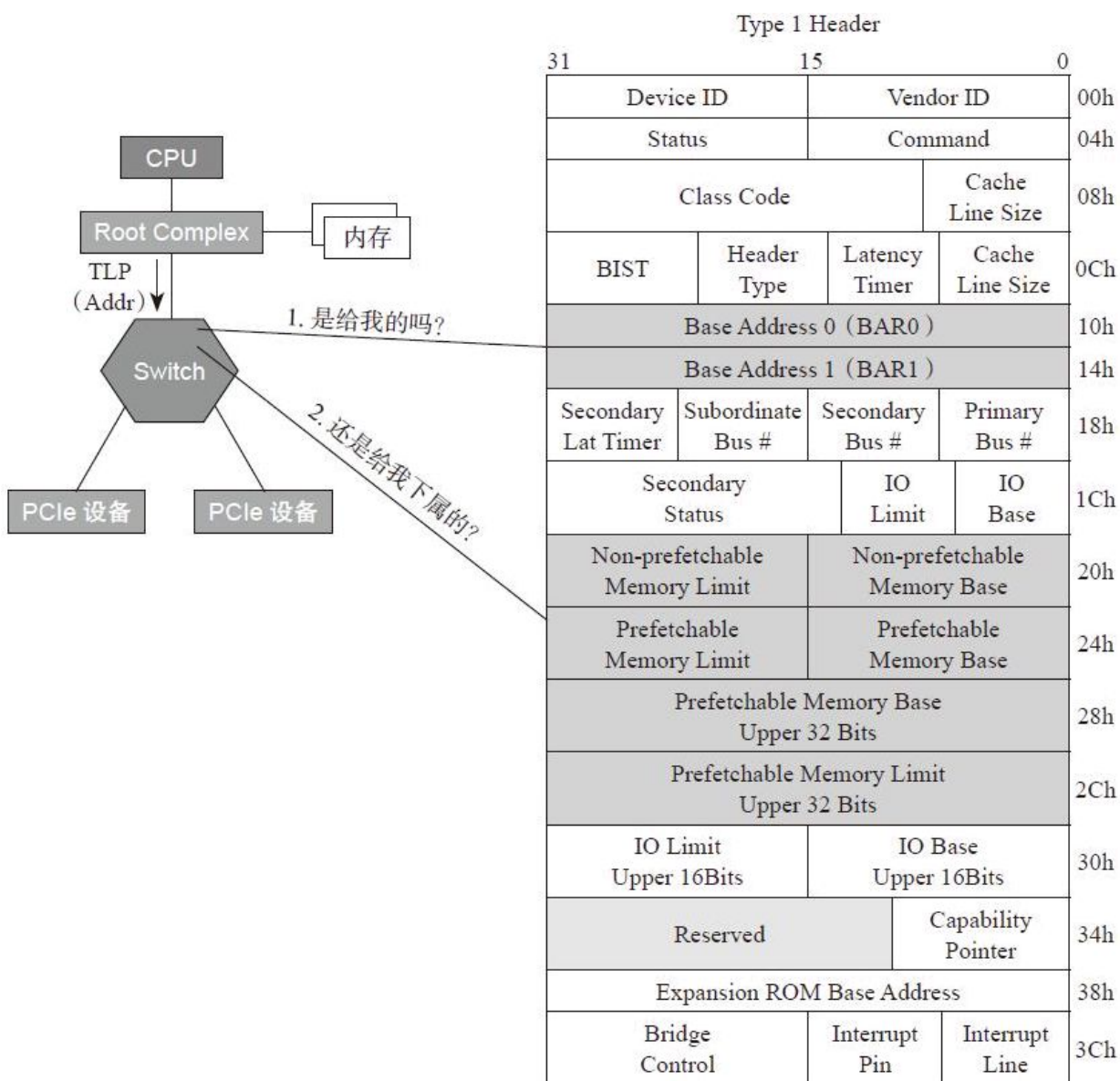


图5-42 Switch如何分配地址路由

2.ID路由

在一个PCIe拓扑结构中，由ID=Bus Number+Device Number+Function Number (BDF) 能唯一找到某个设备的某个功能。这种按设备ID号来寻址的方式叫作ID路由。Configuration TLP和Completion TLP (CplD) 按ID路由寻址，Message在某些情况下也是ID路由。

使用ID路由的TLP，其TLP Header中含有BDF信息（见图5-43）。

当一个Endpoint收到一个这样的TLP，它用自己的ID和收到TLP Header中的BDF比较，如果是给自己的，就收下TLP，否则就拒绝。

如果是一个Switch收到这样的一个TLP，怎么处理？我们再回头看看Switch的Configuration Header（见图5-44）。

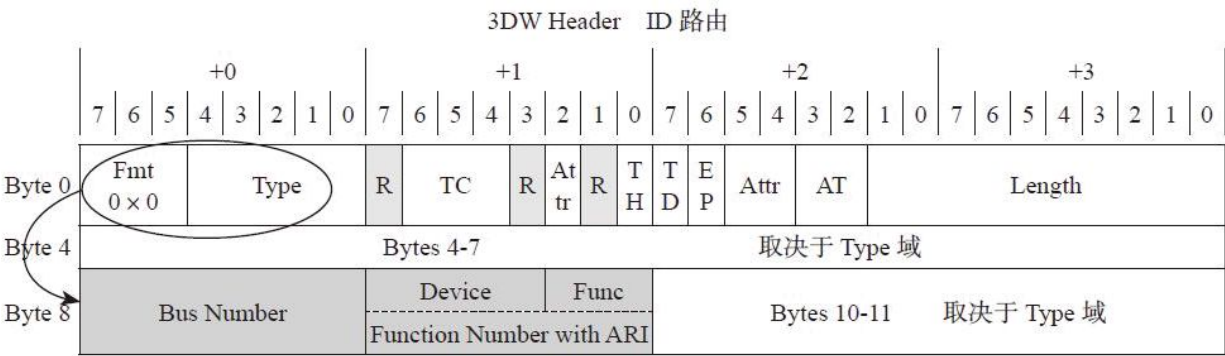


图5-43 使用ID路由的3DW TLP Header

注意： 不是一个Switch对应一个Configuration空间（Type 1Header），而是Switch的每个Port都有一个Configuration空间（Type 1Header）。

Type 1 Header				
31	15		0	
Device ID		Vendor ID		00h
Status		Command		04h
Class Code			Cache Line Size	08h
BIST	Header Type	Latency Timer	Cache Line Size	0Ch
Base Address 0 (BAR0)				10h
Base Address 1 (BAR1)				14h
Secondary Lat Timer	Subordinate Bus #	Secondary Bus #	Primary Bus #	18h
Secondary Status		IO Limit	IO Base	1Ch
Non-prefetchable Memory Limit		Non-prefetchable Memory Base		20h
Prefetchable Memory Limit		Prefetchable Memory Base		24h
Prefetchable Memory Base Upper 32 Bits				28h
Prefetchable Memory Limit Upper 32 Bits				2Ch
IO Limit Upper 16Bits		IO Base Upper 16 Bits		30h
Reserved			Capability Pointer	34h
Expansion ROM Base Address				38h
Bridge Control		Interrupt Pin	Interrupt Line	3Ch

图5-44 Type 1Header

看三个寄存器：Subordinate Bus Number、Secondary Bus Number和Primary Bus Number，如图5-45所示。

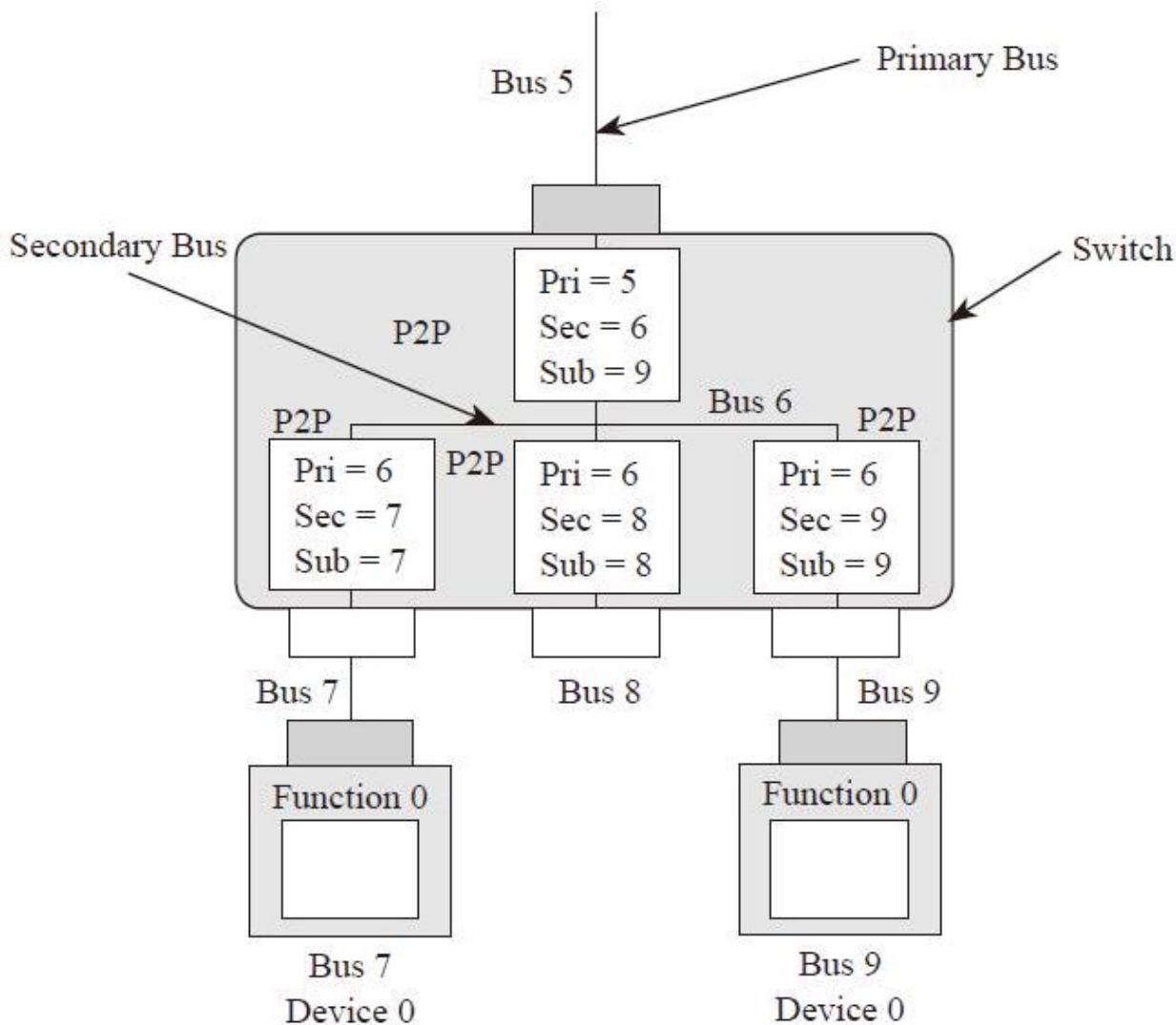


图5-45 Primary Bus和Secondary Bus的概念

对一个Switch来说，每个Port靠近RC（上游）的那根Bus叫作Primary Bus，其Number写在其Configuration Header中的Primary Bus Number寄存器；每个Port下面的那根Bus叫作Secondary Bus，其Number写在其Configuration Header中的Secondary Bus Number寄存器；对上游端口，Subordinate Bus是其下游所有端口连接的Bus编号最大的那根Bus，Subordinate Bus Number写在每个Port的Configuration Header中的Subordinate Bus Number寄存器。

当一个Switch收到一个基于ID寻址的TLP，首先检查TLP中的BDF是否与自己的ID匹配，如匹配，说明该TLP是给自己的，收下；否则，检查该TLP中的Bus Number是否落在Secondary Bus Number和

Subordinate Bus Number之间。如果是，说明该TLP是发给其下游设备的，然后转发到对应的下游端口；如果是其他情况，则拒绝这些TLP。

3.隐式路由

只有Message TLP才支持隐式路由。在PCIe总线中，有些Message是与RC通信的，RC是该TLP的发送者或者接收者，因此没有必要明明白白地指定地址或者ID，这种路由方式称为隐式路由。Message TLP还支持地址路由和ID路由，但以隐式路由为主。

Message TLP的Header总是4DW，如图5-47所示。

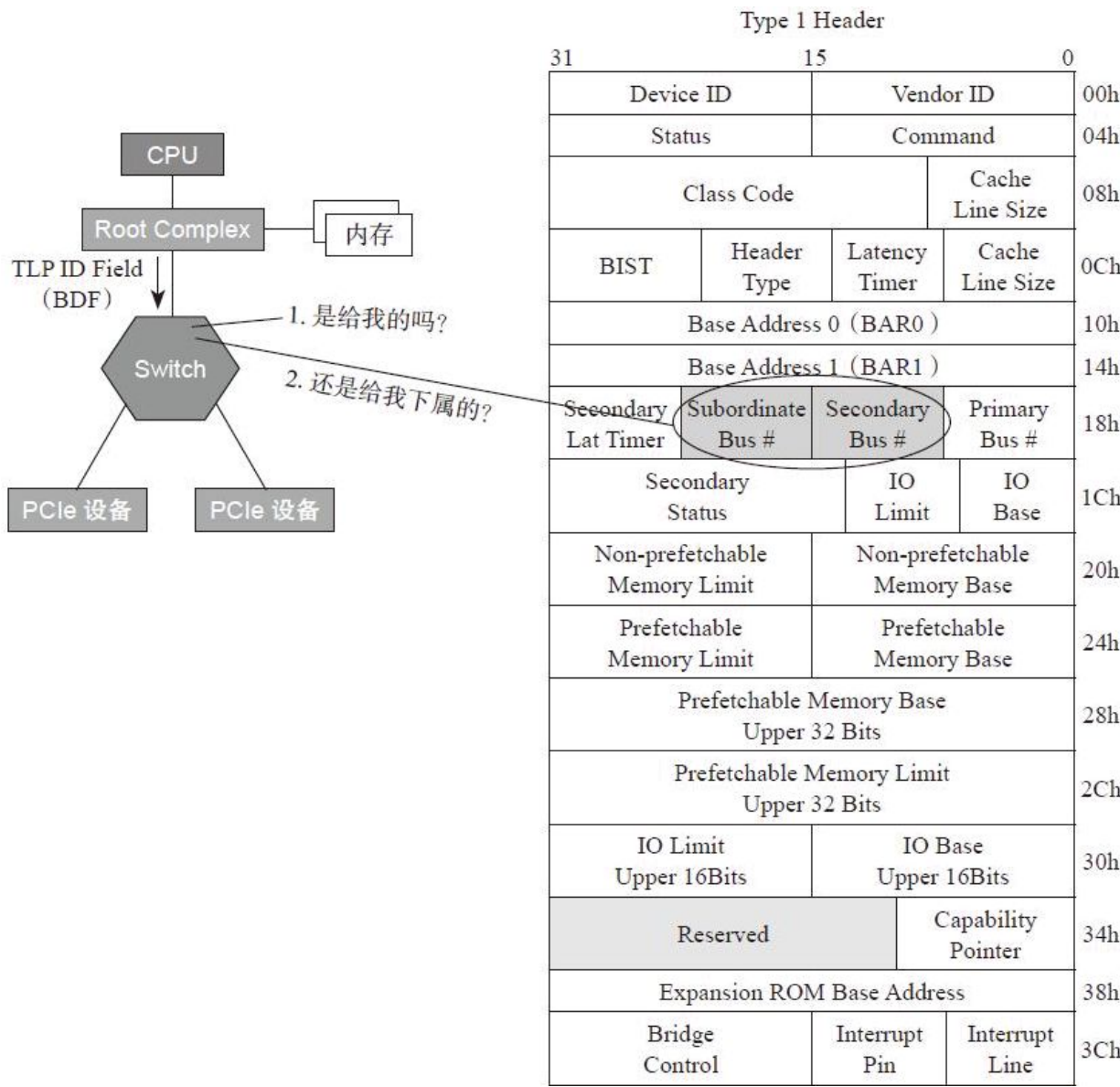


图5-46 Switch如何进行ID路由

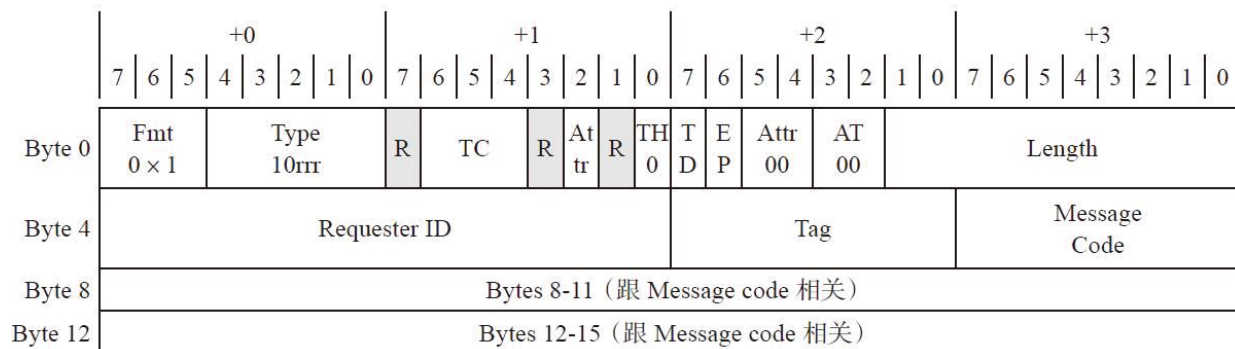


图5-47 Message TLP的Header

Type字段，低3位，由rrr表示，指明该Message的路由方式，具体如图5-48所示。

Message Routing Subfield R[2:0]

- 000b = Implicit - Route to the Root Complex
- 001b = Route by Address (bytes 8-15 of header contain address)
- 010b = Route by ID (bytes 8-9 of header contain ID)
- 011b = Implicit - Broadcast downstream
- 100b = Implicit - Local: terminate at receiver
- 101b = Implicit - Gather & route to the Root Complex
- 110b - 111b = Reserved: terminate at receiver

图5-48 Type域低3位决定了Message TLP路由方式

当一个Endpoint收到一个Message TLP，检查TLP Header，如果是RC的广播Message（011b）或者该Message终结于它（100b），它就接受该Message。

当一个Switch收到一个Message TLP，检查TLP Header，如果是RC的广播Message（011b），则往它每个下游端口复制该Message然后转发。如果该Message终结于它（100b），则接受该TLP。如果下游端口收到发给RC的Message，则往上游端口转发。

上面说的是Message使用隐式路由的情况。如果是地址路由或者ID路由，Message TLP的路由跟其他的TLP一样，不再赘述。

5.8 数据链路层

前面看到，一个TLP源于事务层，终于事务层。但TLP不是从发送端一步就跑到接收端，它经由发送端的数据链路层和物理层，然后是接收端的物理层和数据链路层，最终完成TLP的发送和接收。

数据链路层位于事务层的下一层，理所当然为事务层服务。那么，数据链路层在TLP传输过程中起了什么作用呢？

发送端：数据链路层接收上层传来的TLP，它给每个TLP加上Sequence Number（序列号，下文都用“序列号”来阐述）和LCRC（Link CRC），然后转交给物理层。

接收端：数据链路层接收物理层传来的TLP，检测CRC和序列号，如果有问题，会拒绝接收该TLP，即不会传到它的事务层，并且通知发送端重传；如果该TLP没有问题，数据链路层则去除TLP中的序列号和LCRC，交由它的事务层，并通知发送端TLP正确接收。

从上面的描述可以看出，数据链路层保证了TLP在数据总线上的正常传输，并使用了握手协议（Ack/Nak）和重传（Retry）机制来保证数据传输的一致性和完整性。

数据链路层的作用，除了保证TLP数据包的正确传输，还包括TLP流量控制和电源管理等功能。数据链路层借助DLLP来完成这些功能，如图5-49所示。

DLLP（Data Link Layer Packet，数据链路层的数据包）源于发送端的数据链路层，终于接收端的数据链路层，因此，处于高层的事务层是感知不到它的存在的。

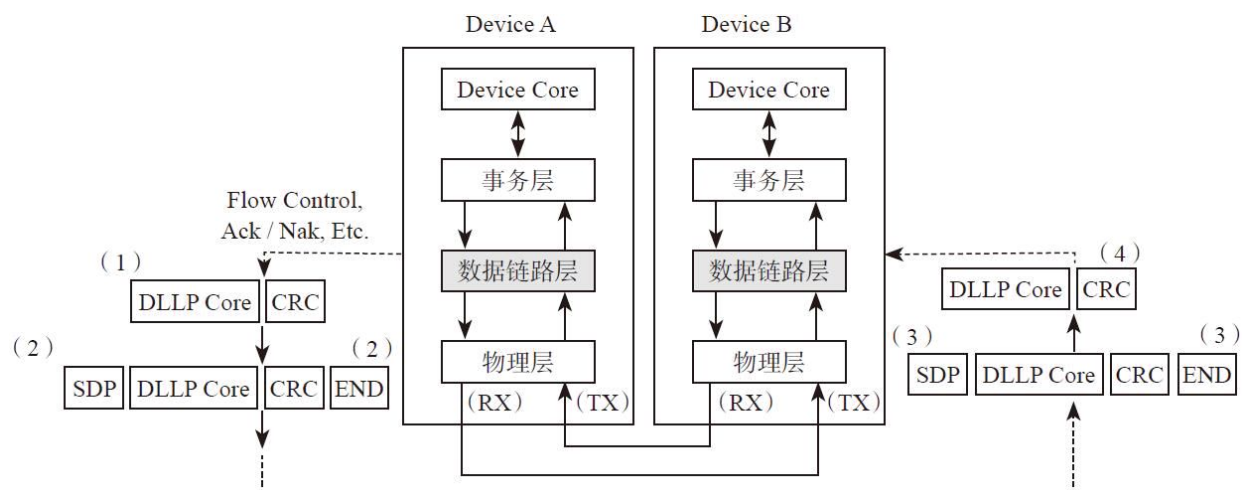


图5-49 数据链路层在协议栈中的位置和作用

发送端：数据链路层生成DLLP，交由物理层，物理层加起始（SDP）和结束标志（GEN 1/2加END，GEN3则没有），然后物理传输到对方。

接收端：物理层对DLLP掐头去尾，交由数据链路层，数据链路层对DLLP进行校验，不管正确与否，DLLP都终于这层。

与事务层TLP传输不同，数据链路层只处理端到端的数据传输。一个TLP，可以翻山越岭（经过若干个Switch），从一个设备传输到相隔很远的设备。但DLLP的传输，仅限于相邻的两个端口。因此，DLLP中不需要包含路由信息，即不需要告诉我这个DLLP是哪个设备发起的，以及要发送给哪个目标设备。

如图5-50所示，一个TLP可以从RC传到EP1，但DLLP的传输只限于RC与Switch上游Port，Switch的上游Port与下游Port，以及Switch下游Port与EP1（或者EP2）。

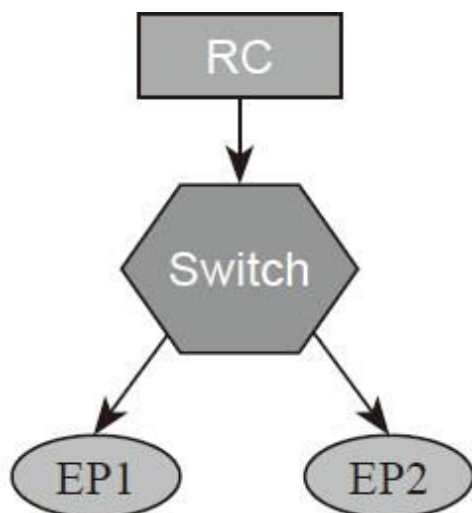


图5-50 简单的PCIe系统示例

数据链路层主要有四大类型DLLP:

- 用以确保TLP传输完整性的DLLP: ACK/NAK;
- 流控相关的DLLP;
- 电源管理相关的DLLP;
- 厂家自定义DLLP。

具体如表5-7所示。

表5-7 DLLP类型

DLLP 类型	类型编码	目的
ACK (确认 TLP 收到无误)	0000 0000b	用以保证 TLP 传输的完整性
NAK (TLP 有问题, 需要重发)	0001 0000b	用以保证 TLP 传输的完整性
PM_Enter_L1	0010 0000b	电源管理
PM_Enter_L2L3	0010 0001b	电源管理
PM_Active_State_Request_L1	0010 0011b	电源管理

(续)

DLLP 类型	类型编码	目的
PM_Request_Ack	0010 0100b	电源管理
InitFC1_P	0100 0xxx b	TLP 的流控
InitFC1_NP	0101 0xxx b	TLP 的流控
InitFC1_Cpl	0110 0xxx b	TLP 的流控
InitFC2_P	1100 0xxx b	TLP 的流控
InitFC2_NP	1101 0xxx b	TLP 的流控
InitFC2_Cpl	1110 0xxx b	TLP 的流控
UpdateFC_P	1000 0xxx b	TLP 的流控
UpdateFC_NP	1001 0xxx b	TLP 的流控
UpdateFC_Cpl	1010 0xxx b	TLP 的流控
VendorSpecific	0011 0000	厂家自定义
保留的	其他	保留

DLLP大小为6B（物理层上加上头尾，传输的是8B），格式如图5-51所示。

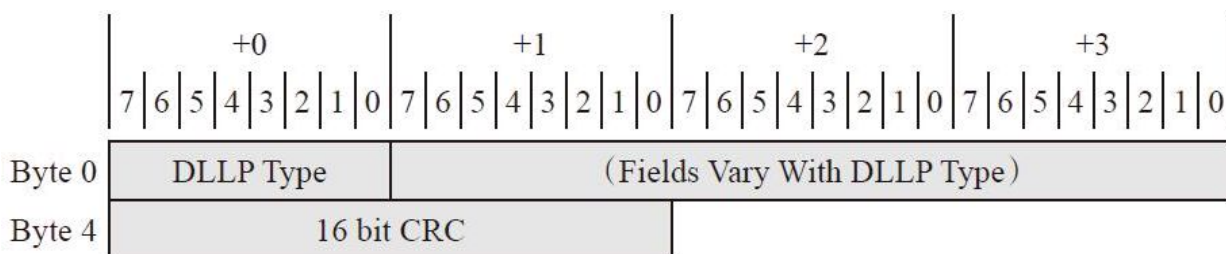


图5-51 6B DLLP格式

不同类型的DLLP，格式相同，内容不一样。

1.ACK/NAK协议

首先，我们来看ACK/NAK DLLP，其格式如下（见图5-52）。

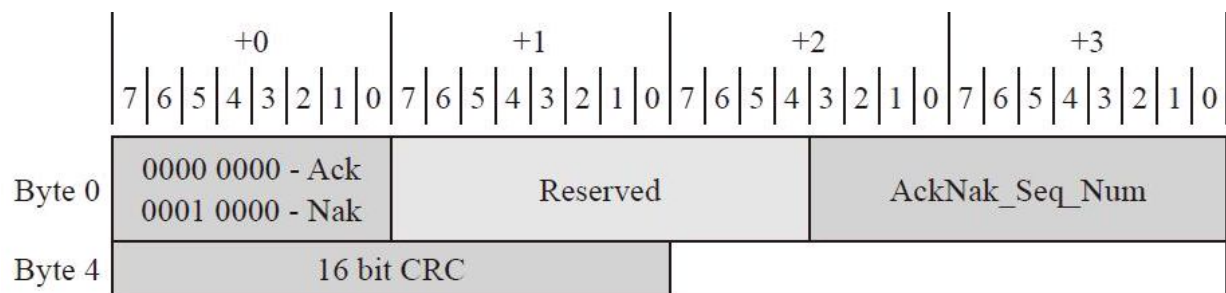


图5-52 ACK/NAK DLLP格式

数据链路层通过ACK/NAK协议来保证每个TLP的正确传输，其基本原理为：TLP发送端的数据链路层为每个TLP加上序列号和LCRC，在该TLP被接收端正确收到之前，它会一直保持在一个叫Replay Buffer的接口里面。TLP接收端的数据链路层接收到该TLP后，做CRC校验和序列号检查，如果没有问题，TLP接收端（可能）会生成和发送ACK DLLP，TLP发送方接收到ACK后，知道TLP被正确接收，因此它会把相关的TLP从Replay Buffer中清除；如果TLP接收方检测到TLP有错误，则会生成和发送NAK DLLP，TLP发送方接收到NAK后，知道有TLP传输出错，会重新发送Replay Buffer相关的TLP给对方。TLP传输出错往往是瞬态的，重传基本能保证TLP传输正确。TLP接收方只有收到正确的TLP才会去掉序列号和LCRC，并把TLP交给它的事务层。

前面提到，没有收到ACK的TLP，发送端的链路层都会把它（包括序列号和LCRC）放在Replay Buffer中。在接收端，当成功收到一个TLP后，它的序列号加1，设置为下一个期望接收到的TLP序列号。

假设当前发送端Replay Buffer中有序列号分别为10、11、12、13的4个TLP，即这些TLP发送出去了，但还没有得到响应。

假设接收端上一个成功接收到的TLP序列号为11，期望下个接收到的TLP序列号为12。这时，接收端接收到一个TLP，首先，它会对该TLP做LCRC校验：

（1）校验失败

TLP接收端会发送一个NAK，其中AckNak_SEQ_NUM设为11。TLP发送端接收到该NAK后，知道11和它之前的TLP（这里是TLP 10）被成功接收，因此TLP 10和TLP 11会从Replay Buffer清掉（不需要重发）。同时，它知道12和后面的TLP（这里是TLP 13）没有被成功接收，因此它们会重发。

（2）校验成功

CRC没有问题，接下来就检查TLP的序列号了。这里有三种情况：

·TLP接收端发现收到的TLP序列号为12，与预期相符。TLP接收端可能需要发一个ACK，也可能不需要发ACK。为什么这么说？为减少数据链路层DLLP的传输，可能设置正确接收到若干个TLP后，才会返回一个ACK，并非每成功接收一个TLP，就返回一个ACK。假设这个

时候需要返回ACK，则设AckNak_SEQ_NUM为12。TLP发送端接收到该ACK，知道TLP 12和它之前所有的TLP都被成功接收，因此TLP 10、TLP 11和TLP 12会从Replay Buffer清掉。

·TLP接收端发现收到的TLP序列号为13，与预期不符（预期为TLP 12）。TLP接收端希望接收到的TLP为12，这个时候收到的却是13，说明TLP 12在半路丢了，发生丢包。这个时候，接收端会发一个NAK，其中AckNak_SEQ_NUM设为11（即上一个成功被接收的TLP序列号）。TLP发送端接收到该DLLP后，知道TLP 11和它之前所有的TLP都被成功接收，因此TLP 10和TLP 11会从Replay Buffer清掉，并重发TLP 12和它后面的TLP（这里是TLP 13）。

·TLP接收端发现收到的TLP序列号为10，与预期不符（预期为TLP 12）。TLP上次正确接收到的是TLP 11，这次又收到一个序列号比它小的TLP，为什么会这样？原因是在TLP发送端，一个TLP在一定时间内没有收到ACK，它会自动重发所有Hold在Replay Buffer中的TLP。由于发送端的这个超时重发机制，导致一个TLP会被接收端接收到两次或者更多次（如果接收端一直不能及时响应）。TLP接收端如果收到重复的TLP包，它会默默扔掉这些重复的TLP，并发送ACK，其中的AckNak_SEQ_NUM设为11。TLP发送端接收到该DLLP后，知道TLP 11和它之前所有的TLP都被成功接收，因此TLP 10和TLP 11会从Replay Buffer清掉。

图5-53是数据链路层内部框图，从中我们可以看到ACK/NAK是怎样实现的。

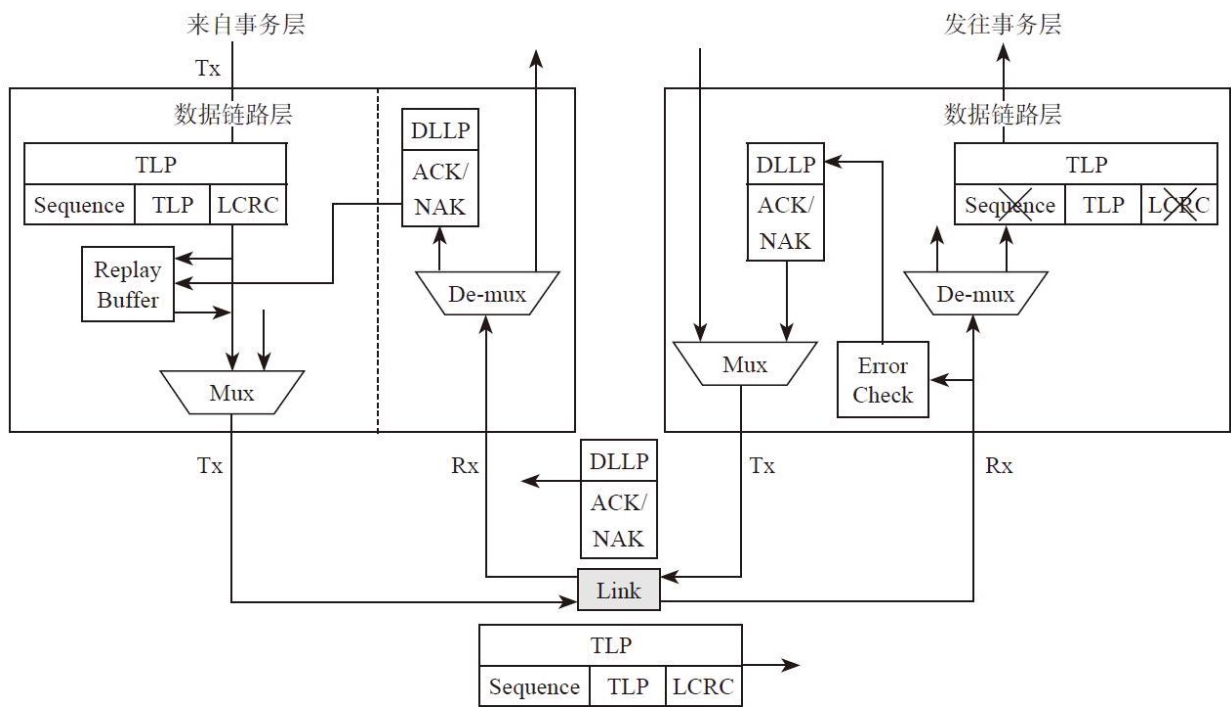


图5-53 数据链路层内部框图

数据链路层通过ACK/NAK协议和TLP重传机制，保障了TLP传输的数据完整性。

问题来了，每个DLLP在接收端也需要做CRC校验，那如果DLLP出错了怎么办？接收端会丢弃出错的DLLP，并通过下一个成功的DLLP更新之前丢失的信息。读者可根据上面的例子自行分析。

2.TLP流控（流量控制，Flow Control）

我们再看看跟流控相关的DLLP，其格式如图5-54所示。

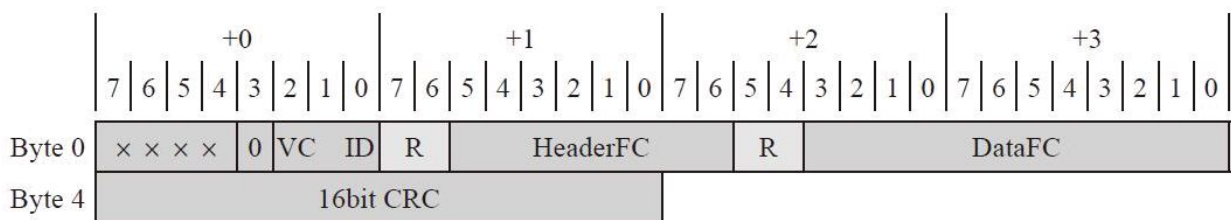


图5-54 流控DLLP格式

我们打算对每个流控DLLP展开解释，这里只简单说说TLP流控机制。

TLP的发送端不能随便向对方发送TLP，因为接收端处理TLP的速度可能赶不上发送TLP的速度。接收端如果没有足够空间接受该TLP的话，就会拒绝该TLP，发送端必须重复发送该TLP直到对方接受，这在一定程度上影响了通信的效率。PCIe有一套流控机制，来保证TLP的发送和接收是高效的。

TLP流控基于Credit。每个TLP都有一定大小，发送者在发送前，先看看对方是否有足够的空间来接纳该TLP，如果有，则发送过去，否则就Hold在那里，直到对方有足够的空间再发。那发送者怎样才能知道对方有多少空间呢？PCIe使用流控DLLP来告知。接收端会时不时通过DLLP来告诉对方我有多少TLP接收空间，然后发送端依据此信息决定是不是生成TLP并发送过去，如图5-55所示。

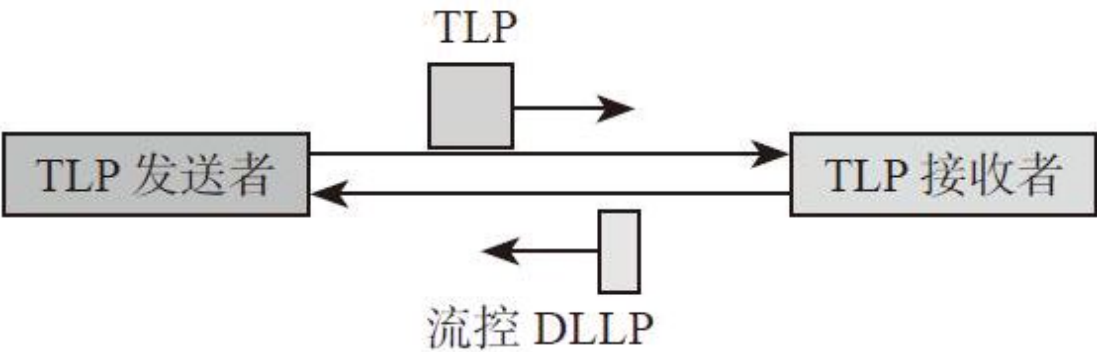


图5-55 TLP接收者通过流控DLLP告知发送者可用TLP接收空间

需要注意的是，这里的流控是针对TLP传输而言。DLLP的传输是不需要流控的，因为每个DLLP的大小只有六个字节，跟TLP相比非常迷你。如果DLLP需要流控，那就麻烦了。TLP的流控是通过DLLP来实现的，如果DLLP还需要流控，那又有谁来帮忙实现呢？

3.电源管理

最后是跟电源管理相关的DLLP（见图5-56）。

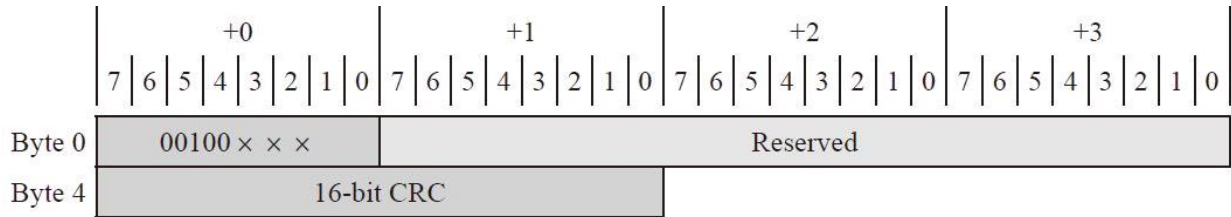


图5-56 电源管理DLLP格式

关于电源管理，请查看第8章，在这里不做解释。

5.9 物理层

物理层是整个PCIe协议层的最底层，用来跑腿的。无论是TLP还是DLLP，到最后都需要物理层来进行实实在在的物理信号传输。因此，有必要深入基层，了解一下物理层在做什么。

物理层由电气模块和逻辑模块组成。电气模块方面，我们知道PCIe是采用串行总线传输数据，使用的是差分信号，即用两根信号线上的电平差表示0或1。与单端信号传输相比，差分信号抗干扰能力强，能提供更宽的带宽（跑得更快）。打个比方，假设用两个信号线上电平差表示0和1，具体来讲，差值大于0，表示1；差值小于0，表示0。如果传输过程中存在干扰，两个线上加了近乎同样大小的干扰电平，两者相减，差值几乎不变，并不会影响信号传输。但对单端信号传输来说，就很容易受干扰，比如0~1V表示0，1~3V表示1，一个本来是0.8V的电压，加入干扰，变成1.5V，相当于0变成1，数据就出错了。抗干扰能力强，因而可以用更快的速度进行数据传输，从而提供更宽的带宽（关于PCIe速度，可参看5.1节）。

关于电气模块更多详细内容，可以去读PCIe规范。对于SSD开发人员（尤其是固件开发者）来说，我觉得记住“串行总线，差分信号”就可以了，PCIe的快是因为在物理传输上使用了这两大技术。

我们重点看看物理层的逻辑模块，如图5-57所示。

来自数据链路层的数据

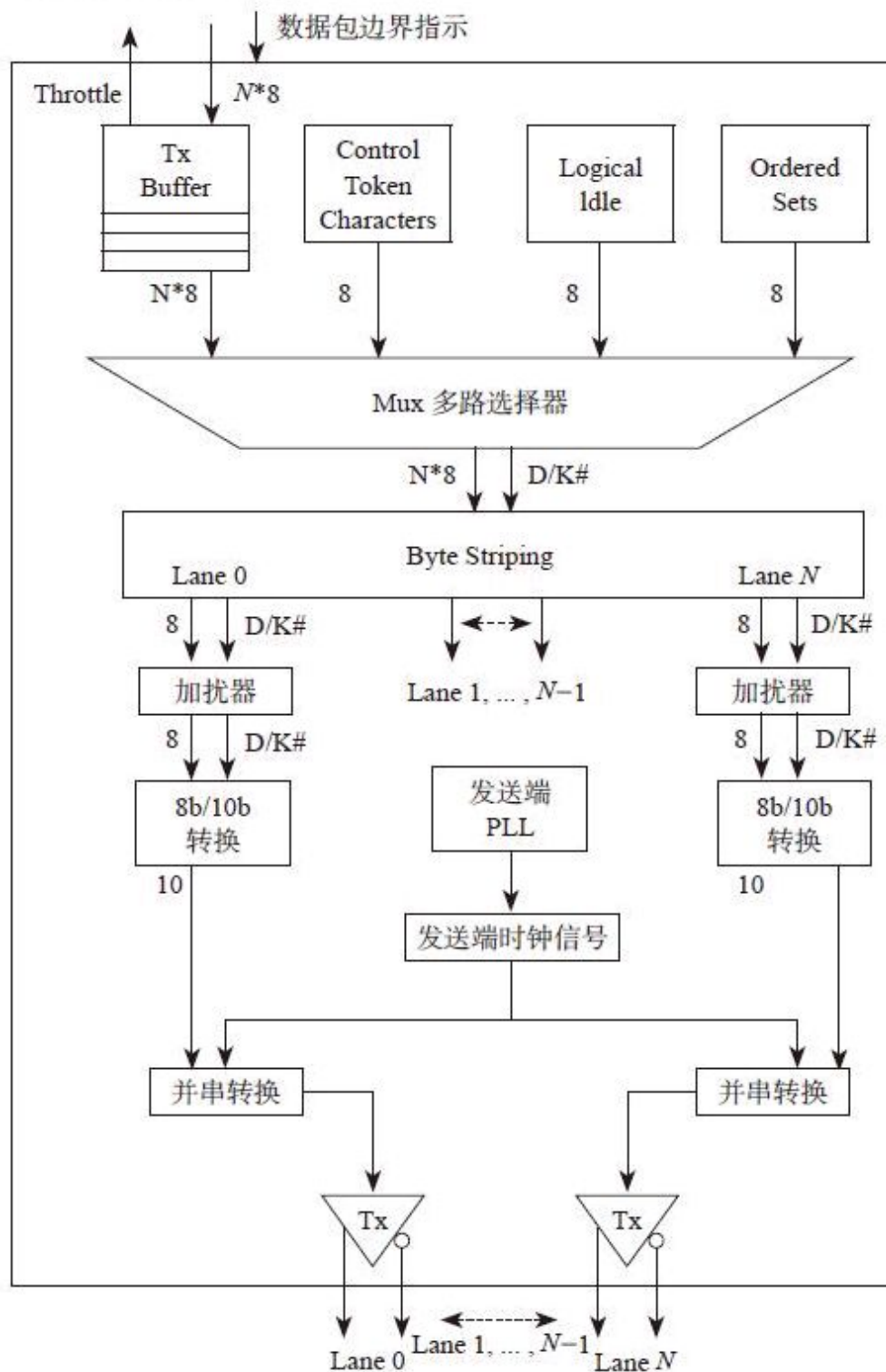


图5-57 物理层中发送端逻辑子模块

·物理层从数据链路层获得TLP或者是DLLP，然后放到TxBuffer里。

·物理层给TLP或者DLLP加入头（Start code）和尾（End code、Gen 3没有尾巴）；给每个TLP或者DLLP加上边界符号，这样接收端就能把TLP或者DLLP区分开。

·第一节提到，PCIe链路上可能有若干个Lane。在物理层，TLP或者DLLP数据会分派到每个Lane上独立传输。这个过程叫Byte Stripping，类似于串并转换。

·数据进入每条Lane后，分别加串扰（Scramble），目的是减少电磁干扰（EMI），手段是让数据与随机数据进行异或操作，输出伪随机数据，然后再发送出去。

·加扰后的数据进行8/10编码（Gen3是128/130编码）。8/10编码是IBM的专利，目的主要有：让数据流中的0和1个数相当，保持直流平衡；嵌入时钟信息，PCIe不需要专门的时钟进行信号传输。

·最后进行并串转换，发送到串行物理总线上去。

接收端逻辑模块如图5-58所示。

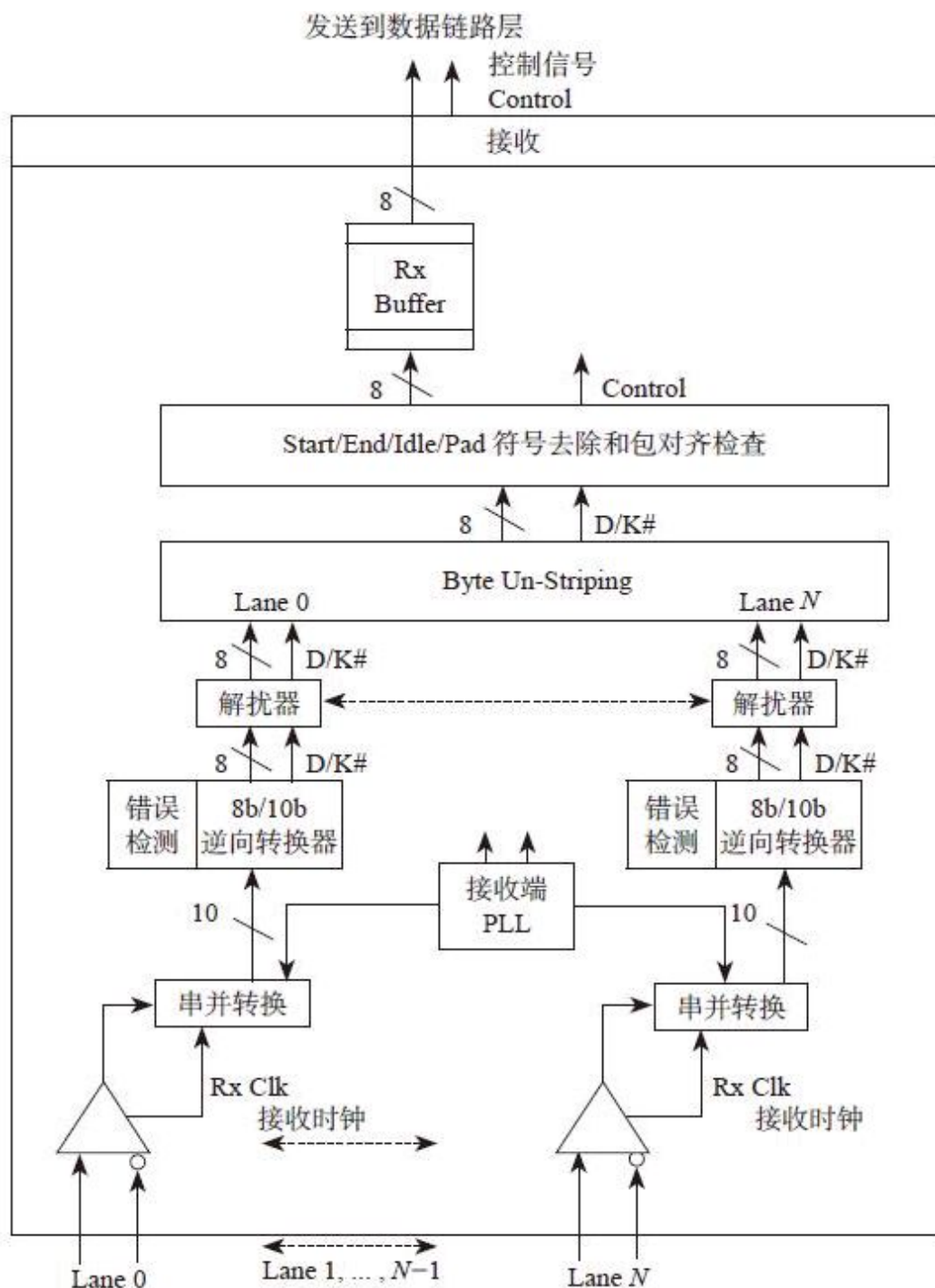


图5-58 物理层中接收端逻辑子模块

接收端逆向操作，不再赘述。

PCIe的三层，从上到下，依次为事务层、数据链路层和物理层。每层都有自己的数据包定义：事务层产生TLP，经过数据链路层和物理

层传输给接收方；数据链路层产生DLLP，经过物理层传输到对方；物理层，不仅仅为上层TLP和DLLP做嫁衣，其实它也有自己的数据包定义，称为Ordered Sets，简称OS。

TLP用以传输应用层或者命令层（事务层的顶头上司）数据，DLLP用以ACK/NAK、流控和电源管理等，OS的功能是物理层用以管理链路的，比如链路训练（LinkTraining）、改变链路电源状态等。表5-8是PCIe中OS列表。

表5-8 Ordered Sets列表

Ordered Sets	说明
TS1OS/TS2OS	Training Sequence，用以链路初始化和链路训练等
EIOS	Electrical Idle，使 PCIe 链路进入空闲状态
FTSOS	Fast Training Sequence，使 PCIe 链路从低功耗状态 (L0s) 进入正常工作状态 (L0)
SOS (SKP OS)	SKP OS，用于时钟补偿
EIEOS	Electrical Idle Exit，PCIe 链路退出空闲状态

5.10 PCIe Reset

PCIe是个博大精深的协议，跟Reset相关的术语就有不少：Cold Reset、Warm Reset、Hot Reset、Conventional Reset、Function Level Reset、Fundamental Reset、Non-Fundamental Reset。

要想完全理解PCIe Reset，就要提纲挈领，快速从一大堆概念中理出头绪。

1.整理出这些Reset之间的关系

这些Reset之间是从属关系，总线规定了两个复位方式：Conventional Reset和Function

Level Reset（FLR）。

而Conventional Reset又进一步分为两大类：Fundamental Reset和Non-Fundamental Reset。

Fundamental Reset方式包括Cold和Warm Reset方式，可以用PCIe将设备中的绝大多数内部寄存器和内部状态都恢复成初始值。

而Non-Fundamental Reset方式为Hot Reset方式。

看看表5-9，有没有感觉好一点？

表5-9 PCIe Reset分类

Conventional Reset	Fundamental Reset	Cold Reset 和 Warm Reset
	Non-Fundamental Reset	Hot Reset
Function Level Reset		

2.明白每种Reset的功能、实现方式及对设备的影响

Fundamental Reset: 由硬件控制，会重启整个设备，包括：重新初始化所有的State Machine、所有的硬件逻辑、Port State和Configuration Register。

当然，也有Fundamental Reset搞不定的情况，就是某些Register里属性为“Sticky”的Field，跟蛋蛋一样坚强，任你怎么Reset，我自岿然不动。

这些Field在Debug的时候非常有用，特别是那些需要Reset Link的情况，比如在Link Reset以后还能保存之前的错误状态，这对FW以及上层应用来说是很有用的。Fundamental Reset一般发生在整个系统Reset的时候（比如重启电脑），但是也可以只针对某个设备做Fundamental Reset。

Fundamental Reset有两种：

- Cold Reset: Power Off/On Device的Vcc（Vaux一直在）。

- Warm Reset（Optional）：保持Vcc的情况下由系统触发，比如改变系统的电源管理状态可能会触发设备的Warm Reset，PCIe协议没有定义具体如何触发Warm Reset，而是把决定权交给系统。

有两种方法对一块PCIe SSD做Fundamental Reset。

系统这边给设备发PERST#（PCIe Express Reset）信号，以图5-59所示为例。

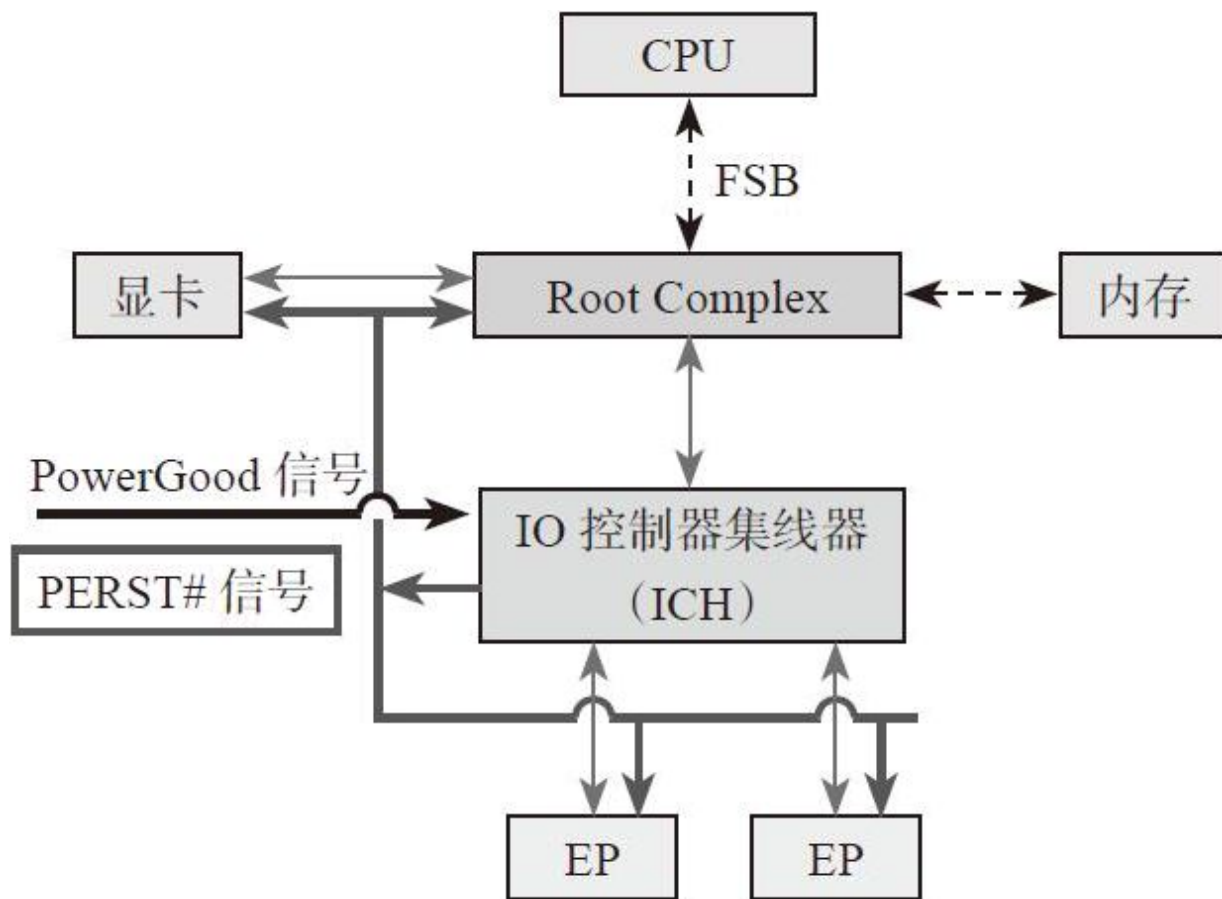


图5-59 系统上电产生PERST#信号

1) 如果这块PCIe设备支持PERST#信号:

·一个系统上电时, 主电源稳定后会有“Power Good”信号;

·这时ICH就会发PERST#信号给下面挂的PCIe SSD;

·如果系统重启, Power Good信号的变化会触发PERST#的Assert和De-Assert, 就可以实现PCIe设备的Cold Reset;

·如果系统可以提供Power Good信号以外的方法触发PERST#, 就可以实现Warm Reset, PERST#信号会发送给所有PCIe设备, 设备可以选择使用这个信号, 也可以不理它;

2) 如果这块PCIe设备不支持PERST#信号:

·上电时它会自动进行Fundamental Reset;

·那些特立独行，选择不理睬PERST#信号的设备，必须能自己触发Fundamental Reset。比如，侦测到3.3V后就触发Reset（当设备发现供电超过其标准电压时，必须触发Reset）。

Hot Reset: 通过Assert TS1的Symbol 5的Bit[0]实现（见图5-60）。

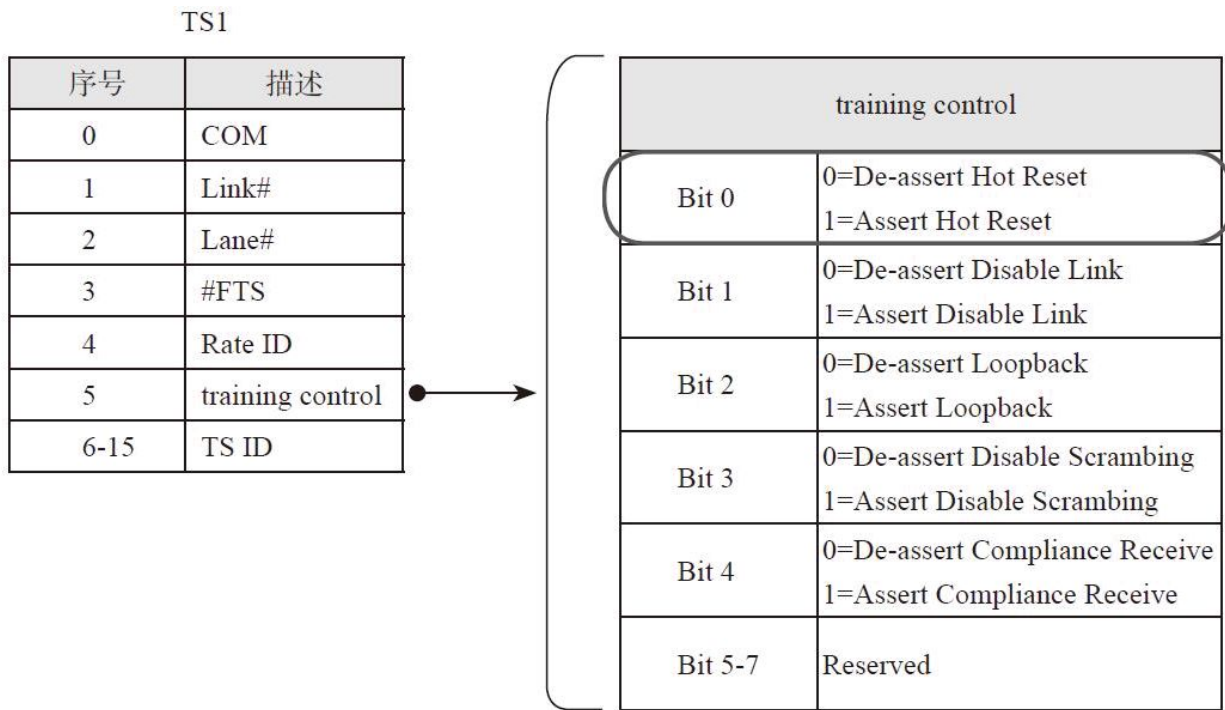


图5-60 TS1中的Hot Reset控制位

PCIe设备收到两个连续的带Hot Reset的TS1后，经过2ms的timeout:

- LTSSM经过Recovery和Hot Reset State，最终停在Detect State（Link Training的初始状态）；
 - 设备所有的State Machine、硬件逻辑、Port State和Configuration Register（Sticky bit除外）全部回到初始值。
- 当PCIe SSD出现问题时，可以通过软件触发Hot Reset使其恢复，具体方法如下：
- 对RC的Bridge Control Register Bit[6]–Secondary Bus Reset写“1”；
 - RC会开始发带Hot Reset的TS1；

·2ms后设备会进入Hot Reset状态，此时LTSSM的状态变化是L0 → RCVRY → HOTRESET；

·将RC的Bridge Control Register Bit[6]–Secondary Bus Reset清零，设备的LTSSM的状态变化HOTRESET → DETECT；

·重新开始LTSSM进行Link Training。

这个我觉得有点像SATA里面主机端通过Trigger OOB去修复Link上的一些问题。

软件还可以通过设置设备的Link Control Register（链路控制寄存器）–Link disable bit把设备disable掉（见图5-61）。

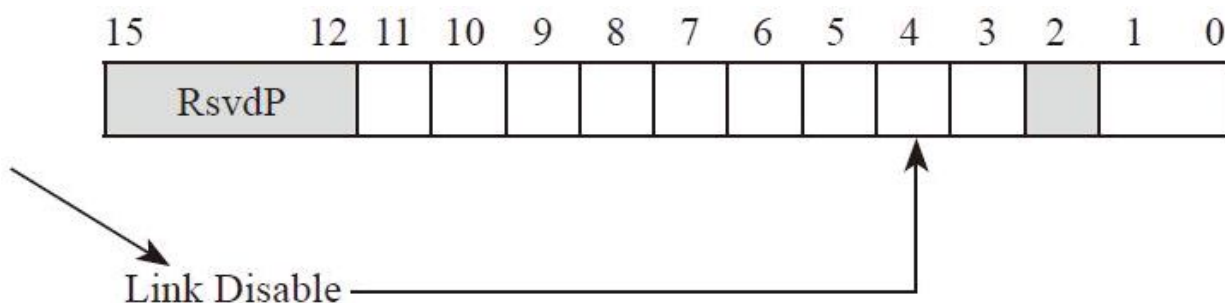


图5-61 PCIe链路控制寄存器

当设备的Link Disable bit被置上以后，会进入LTSSM Recovery State，开始向RC发送带Disable bit的TS1（这个动作只能由EP发起，RC端这个bit是reserve的），如图5-62所示。

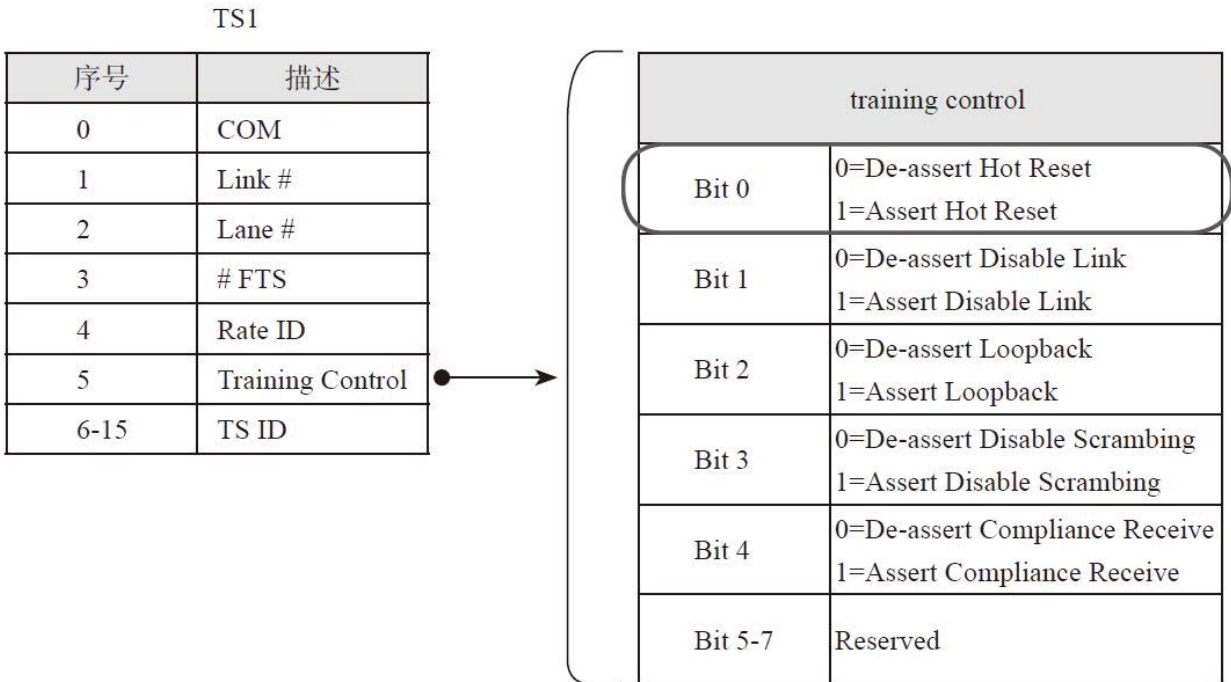


图5-62 TS1中的Disable Link控制位

RC端收到这样的TS1以后，其物理层会发送LinkUp=0的信号给链路层，之后所有的Lane都会进入Electrical Idle。2ms timeout后，RC会进入LTSSM Detect mode，但是设备会一直停留在LTSSM的Disable状态，等待重出江湖的那一天。

FLR (Function Level Reset)：PCIe Link就像一条大马路，上面可以跑各种各样的车，这些车就是不同的Function。如果某个Function出了问题，当然可以通过Reset整个Link的方式来解决，不过细腻的阿呆不会建议采取这种方法，他会使用Function Level Reset，哪里不舒服点哪里。并不是所有的设备都支持FLR，需要检查Device Capabilities Register（设备能力寄存器）的Bit28进行确认。

如果设备支持FLR，那么软件就可以通过Device Control Register（设备控制寄存器）的Bit15来进行Function Reset了，（见图5-64）。

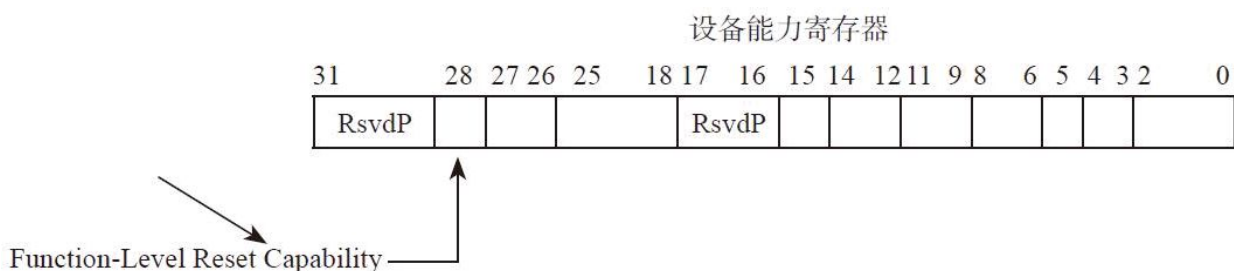


图5-63 设备能力寄存器

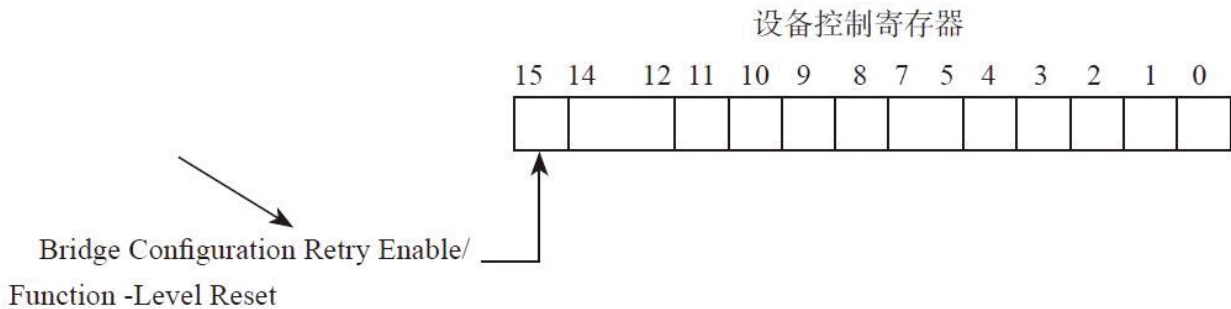


图5-64 设备控制寄存器

FLR会把对应Function的内部状态，寄存器重置，但是以下寄存器不会受到影响：

- Sticky bits——Cold Reset和Warm Reset都拿它们没辙。

- HwInit类型的寄存器。在PCIe设备中，有效配置寄存器的属性为HwInit，这些寄存器的值由芯片的配置引脚决定，后者上电复位后从EEPROM中获取。Cold Reset和Warm Reset可以复位这些寄存器，然后从EEPROM中重新获取数据，但是使用FLR方式不能复位这些寄存器。

- 一些特殊的配置寄存器。比如Captured Power、ASPM Control、Max_Payload_Size或者Virtual Channel。

- FLR不会改变设备的LTSSM状态。

FLR的时间：协议规定一个Function的Reset需要在100ms内完成。但是软件在启动FLR前，要注意是否有还没完成的CplID，遇到这种情况，要么等这些CplID完成再开始FLR，要么启动FLR以后等100ms以后再重新初始化这个Function。这种情况如果不处理好，可能会导致Data Corruption——前一批事务要求的数据因为FLR的影响被误传给了后一批事务。

要避免这种情况，阿呆建议这么做：

- 确保其他软件在FLR期间不会访问这个Function；

- 把Command Register清空，让Function自己待着；

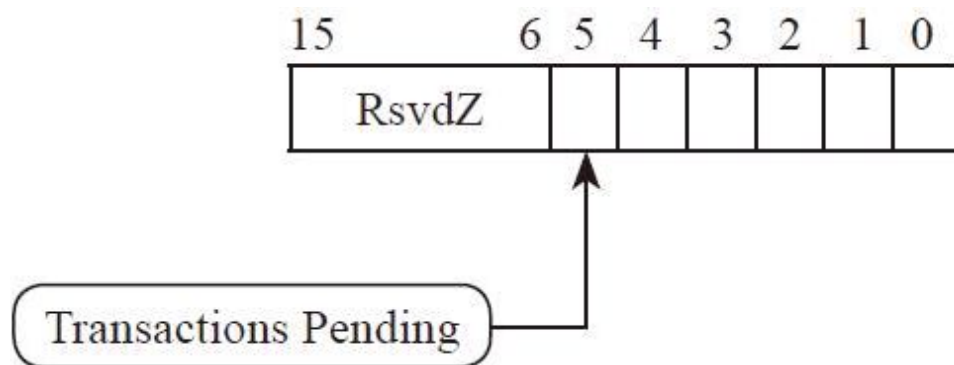


图5-65 设备状态寄存器

·轮循Device Status Register（设备状态寄存器）的bit5（Transactions Pending）直到被Clear（这个bit=1代表还有未完成的CplD），如图5-65所示，或者等待到Completion Timeout的时间，如果Completion Timeout没有被Enable，等100ms；

- 初始化FLR然后等100ms；
- 重新配置Function并Enable。

在FLR过程中：

- 这个Function对外不能被使用；
- 不能保留之前的任何可以被读取的信息（比如内部的Memory需要被清零或者改写）；
- 回复要求FLR的Cfg Request，并开始FLR；
- 对于发进来的TLP可以回复UC（Unexpected Completion）或者直接丢掉；
- FLR应该在100ms之内完成，但是其后的初始化还需要花一些时间，在初始化过程中如果收到Cfg Request，可以回复CRS（Configuration Retry Status）。

阿呆总结了Reset退出时的那些事：

- 从Reset状态退出后，必须在20ms内开始Link Training；

- 软件需要给Link充分的时间完成Link Training和初始化，至少要等上100ms才能开始发送Cfg Request;

- 如果软件等了100ms开始发Cfg Request，但是设备还没初始化完成，设备会回复CRS;

- 这时RC可以选择重发Cfg Request或者上报CPU说设备还没准备好;

- 设备最多可以有1s时间（从PCI那继承来的），之后必须能够正常工作，否则System/RC则可以认为设备挂了。

5.11 PCIe Max Payload Size和Max Read Request Size

我们来聊两句MAX_READ_REQUEST_SIZE和MAX_PAYLOAD_SIZE。

这两部分都在Device Control Register（设备控制寄存器）里，如图5-66所示，分别由bit[14:12]和bit[7:5]控制。

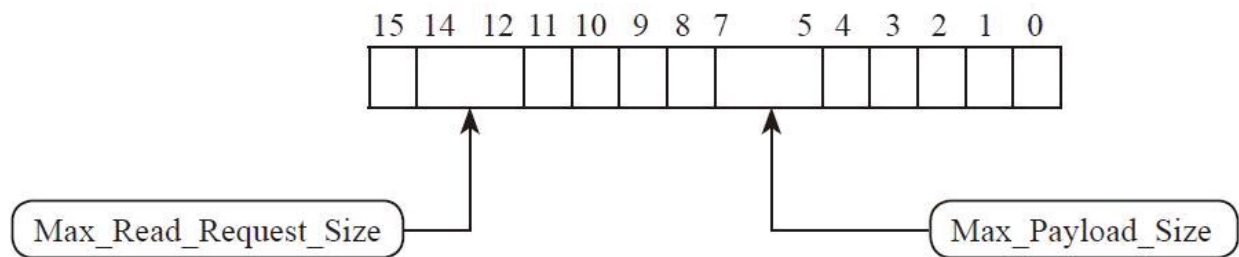


图5-66 设备控制寄存器

1.Maximum Payload Size（简称MPS）

控制一个TLP可以传输的最大数据长度。作为接收方，必须能处理跟MPS设定大小相同的TLP数据包，作为传输方，不允许创建超过MPS设定的TLP数据包。

PCIe协议允许一个最大的Payload可以到4KB，但是规定了在整个传输路径上的所有设备，都必须使用相同的MPS设置，同时不能超过该路径上任何一个设备的MPS能力值。也就是说，MPS Capability高的设备要迁就低的设备。以PCIe SSD来说，插到一块老掉牙的主板上（MPS只有128Byte），你的Payload Size再大，也是没有用的。

系统的MPS值设置是在上电以后的设备枚举配置阶段完成的，以主板上的PCIe RC和PCIe SSD为例，它们都在Device Capability Register里声明自己能支持的各种MPS，OS的PCIe驱动侦测到他们各自的能力值，然后挑低的那个设置到两者的Device Control Register中。

PCIe SSD自身的MPS capability则是在其PCIe core初始化阶段设置的。

2.Maximum Read Request Size

在配置阶段，OS的PCIe驱动也会配置另外一个参数Maximum Read Request Size，用于控制一个Memory Read的最大Size，最大4KB（以128Byte为单位）。

Read Request Size是可以大于MPS的，比如给一个MPS=128Byte的PCIe SSD发一个512Byte的Read Request，PCIe SSD可以通过返回4个128Byte的Cpld，或者8个64Byte的Cpld来完成这个Request的响应。OS层面可以通过控制PCIe SSD的Maximum Read Request Size参数，平衡多个PCIe SSD之间的吞吐量，避免系统带宽（总共40个Lane）被某些SSD霸占。

同时，Read Request Size也对PCIe SSD的Performance有影响，这个Size太小，意味着同样的Data，需要发送更多的Request去获取，而Read Request的TLP是不带任何Data Payload的。

举例来说，要传64KB的数据，如果Read Request=128Byte，则需要512个Read TLP，512个TLP的开销可不小的。

为了提高特别是大Block Size Data的传输效率，可以尽量把Read Request Size设得大一点，用更少的次数传递更多的数据。

5.12 PCIe SSD热插拔

PCIe SSD最早是Fusion-IO推出来的，以闪存卡的形式被互联网公司和数据中心广泛使用。闪存卡一般作为数据缓存来使用，如果要在服务器中集成更多的PCIe SSD，闪存卡的形式就有局限了。闪存卡有以下缺点：

- 插在服务器主板的PCIe插槽上，数量有限。
- 通过PCIe插槽供电，单卡容量受到限制。
- 在PCIe插槽上，容易出现由于散热不良导致宕机的问题。

·不能热插拔。如果发现PCIe闪存卡有故障，必须要停止服务，关闭服务器，打开机箱，拔出闪存卡。这对有成百上千台服务器的数据中心来说，管理成本非常高。

所以，如图5-67所示，PCIe SSD推出了新的硬件形式SFF-8639，又称U.2。U.2PCIe SSD类似于传统的盘位式SATA、SAS硬盘，可以直接从服务器前面板热插拔。

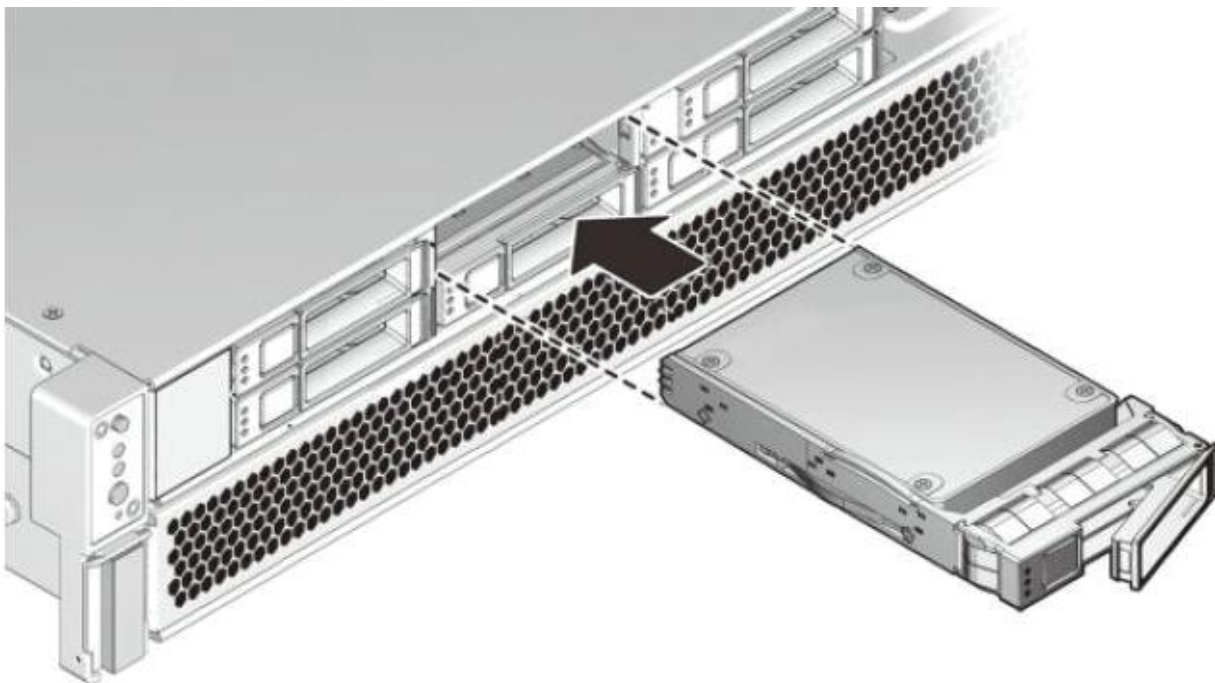


图5-67 热插拔示意图（本图来源于Oracle NVMe SSD热插拔说明）

当服务器有很多个可以热插拔的U.2SSD之后，存储密度大为提升，更重要的是，U.2SSD不只可以用作数据缓存，关键数据也可以放在其中。通过多个U.2SSD组成RAID阵列，当某个U.2SSD故障之后，可以通过前面板显示灯确定故障SSD盘位，予以更换。同时，不会造成服务器停止服务或者数据丢失。

目前有很多服务器厂商都发布了有很多U.2SSD盘位的服务器，有的是少数U.2SSD和多数SATA HDD混合，有的甚至是24个纯U.2SSD盘位。配备了高密度SSD的服务器对数据中心来说，可以大幅减少传统服务器的数量，因为很多企业应用对存储容量要求并不高，传统机械硬盘阵列的容量很大，却处于浪费状态。企业对硬盘带宽的要求更高，一台SSD阵列服务器能够支持的用户数是HDD阵列服务器的好几倍，功耗和制冷成本却少了好几倍。目前，房租和土地成本越来越高，能够在有限的数据中心空间中为大量用户提供服务，对电信、视频网站、互联网公司等企业来说非常重要。所以可以预期，随着闪存价格的逐年下降，配备SSD阵列的服务器会越来越普及。

我们来看看PCIe SSD热插拔的技术实现。传统SATA、SAS硬盘通过HBA和主机通信，所以也是通过HBA来管理热插拔。但是，PCIe SSD直接连到CPU的PCIe控制器，热插拔需要驱动直接管理。根据Memblaze公司公众号的介绍，一般热插拔PCIe SSD需要几方面的支持：

- PCIe SSD：一方面需要硬件支持，避免SSD在插盘过程中产生电流波峰导致器件损坏；另一方面，控制器要能自动检测到拔盘操作，避免数据因掉电而丢失。

- 服务器背板PCIe SSD插槽：需要通过服务器厂家了解是否支持U.2SSD热插拔。

- 操作系统：要确定热插拔是操作系统还是BIOS处理的，也需要咨询服务器主板厂家来确定。

- PCIe SSD驱动：不管是Linux内核自带的NVMe驱动，还是厂家提供的驱动，都需要在各种使用环境中做过大量热插拔稳定性测试，避免在实际操作中因为驱动问题导致系统崩溃。

拔出PCIe SSD的基本流程如下：

- 1) 配置应用程序，停止所有对目标SSD的访问。如果某个程序打开了该SSD中的某个目录，也需要退出；
- 2) `umount`目标SSD上的所有文件系统；
- 3) 有些SSD厂家会要求卸载SSD驱动程序，从系统中删除已注册的块设备和disk；
- 4) 拔出SSD。

5.13 SSD PCIe链路性能损耗分析

下面介绍PCIe SSD在PCIe协议层面导致性能损耗的因素。

1.Encode和Decode

这个就是我们通常说的8/10转换（Gen3是128/130，但是道理一样），简单来说就是对数据重新编码，从而保证链路上实际传输的时候“1”和“0”的总体比例相当，且不要过多连续的“1”或“0”。同时把时钟信息嵌入数据流，避免高频时钟信号产生EMI的问题。Gen1或者Gen2，正常的1个Byte数据，经过8bit/10bit转换在实际物理链路上传输的时候就变成了10bit，也就是一个Symbol，8bit/10bit转换会带来20%的性能损耗。对Gen3，由于是128/130编码，这部分性能损耗可以忽略。

2.TLP Packet Overhead

PCIe SSD通过MemWr或者CplD这两种TLP与主机传输数据，从图5-68中可以看出，整个TLP里Payload是有效的传输Data，而PCIe协议在外面穿了一层又一层的衣服，Transaction Layer（事务层或传输层）、Link Layer（链路层）和PHY（物理层）分别在数据包（Payload）外增加了不少东西。PCIe必须靠这些东西来保证传输的可靠性。

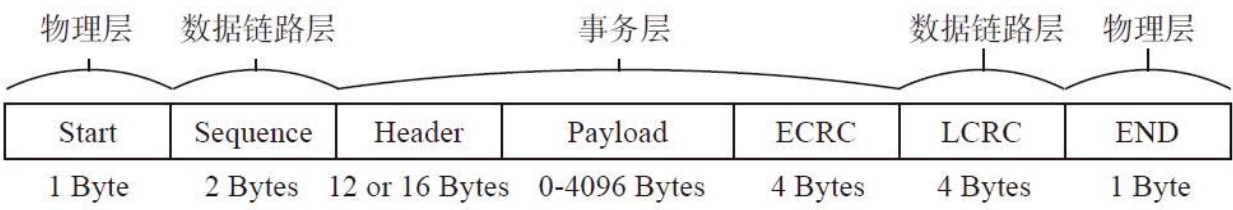


图5-68 PCIe 2.0TLP格式

Transaction Layer: TLP Header、ECRC; Data Link Layer: Sequence、LCRC; PHY Layer: Start、End这些七七八八的加起来，大概每个TLP会带来20~30Byte的额外开销。

3.Traffic Overhead

PCIe协议为了进行时钟偏差补偿，会发送Skip，作用有点像SATA协议的ALIGN。Gen1/Gen2一个Skip是4Byte，Gen3是16Byte，Skip是定期发送的，以Gen2为例，每隔1538个symbol time（symbol time就是PCIe Link上发送一个Byte需要花费的时间）就必须发一个。PCIe协议不允许在TLP中间插入Skip Order-set，只能在两个TLP的间隔中间发，这也会带来损耗。

4.Link Protocol Overhead

PCIe是个有态度的协议，RC（主机）和EP（PCIe SSD）之间发送的每一个TLP，都需要对方告知接收的情况。

以主机传输数据给SSD为例：

- 主机发送一个MemWr的TLP以后，会把这个TLP存在自己这边Data Link Layer Replay Buffer里，同时等SSD回复。
- SSD收到这个TLP以后，如果没问题，就回复ACK。
- 主机收到ACK以后就知道Replay Buffer备份的TLP没用了，可以用后续的TLP覆盖。
- SSD收到TLP如果发现有问题，比如说LCRC错误，就回复NAK。
- 主机收到NAK以后就把Replay Buffer里的TLP拿出来，再发给SSD一次。
- SSD再检查，然后再回复ACK。

有态度是要付出代价的，ACK和NAK的发送本身也会造成性能损耗，另外这里还要一个平衡需要掌握：PCIe要求每一个TLP，都需要对方发送ACK确认，但是允许对方接收几个TLP以后再发一个ACK确认，这样可以减少ACK发送的数量，对性能有所帮助。但是这个连续发送TLP的数量也不能太多，因为Replay buffer是有限的，一旦满了后面的TLP就不能发送了。

5.Flow control

PCIe是个有腔调的协议，自带一个流控机制，目的是防止接收方 receiver buffer overflow。

RC跟EP之间通过交换一种叫UpdateFC的DLLP来告知对方自己目前receive buffer的情况，显然发送这个也会占用带宽，从而对性能产生影响。

跟ACK类似，UpdateFC的发送需要考虑频率问题，更低的频率对性能有好处，但是要求设备有较大的receiver buffer。

6.System Parameters

System Parameters主要有三个，MPS（Max Payload Size）、Max Read Request Size和RCB（Read Completion Boundary），前两个前面已经介绍过了，这里简单说一下RCB。

看PCIe Trace时候，经常遇到的情况是，PCIe SSD向主机发了一个MemRd的TLP要求数据，虽然MPS是256Byte甚至是512Byte，结果主机回复了一堆的64Byte或者128Byte的CplD。

导致这个情况的原因就是RCB，RC允许使用多个CplD回复一个Read Request，而这些回复的CplD通常以64Byte或128Byte为单位（也有32Byte的），原则就是在Memory里做到地址对齐。

研究完这些因素，需要量化计算。

下面用一个公式说明：

$$\text{Bandwidth} = [(\text{Total Transfer Data Size}) / (\text{Transfer Time})]$$

已知条件：

- 200个MemWr TLP;
- MPS=128;
- PCIe Gen1x8。

准备活动：

- 计算Symbol Time，2.5Gbps换算成1个Byte传输时间是4ns；
- 8个Lane，所以每4ns可以传输8个Byte；
- TLP传输时间： $[(128\text{Bytes Payload} + 20\text{Byte overhead}) / 8\text{Byte/Clock}] \times [4\text{ns/Clock}] = 74\text{ns}$ ；
- DLLP传输时间： $[8\text{Bytes} / 8\text{Byte/Clock}] \times [4\text{ns/Clock}] = 4\text{ns}$ 。

假设：

- 每5个TLP回复1个ACK；
- 每4个TLP发送一个FC Update。

正式计算：

- 总共的数据： $200 \times 128\text{Byte} = 25600\text{Byte}$ ；
- 传输时间： $200 \times 74\text{ns} + 40 \times 4\text{ns} + 50 \times 4\text{ns} = 15160\text{ns}$ ；
- 性能： $25600\text{Bytes} / 15160\text{ns} = 1689\text{MB/s}$ 。

可将MPS调整到了512B。重新计算，结果增加到了1912MB/s，看到这个数字可知，以前的SATA SSD可以退休了。

以上的例子是以MemWr为例，而使用MemRd的时候，情况略有不同：MemWr的TLP自带Data Payload，而MemRd是先发一个Read Request TLP，而后对方回复CplD进行Data传输，而CplD Payload的Size则会受到RCB的影响。

第6章 NVMe介绍

6.1 AHCI到NVMe

HDD和早期的SSD绝大多数都是使用SATA接口，跑的是AHCI（Advanced Host Controller Interface），它是由Intel联合多家公司研发的系统接口标准。AHCI支持NCQ（Native Command Queuing）功能和热插拔技术。NCQ最大深度为32，即主机最多可以发32条命令给HDD或者SSD执行，跟之前硬盘只能逐条命令执行相比，硬盘性能大幅提升。

在HDD时代或者SSD早期，AHCI协议和SATA接口足够满足系统性能需求，因为整个系统的性能瓶颈在硬盘端（低速，高延时），而不是在协议和接口端。然而，随着SSD技术的飞速发展，SSD盘的性能飙升，底层闪存带宽越来越宽，介质访问延时越来越低，系统性能瓶颈已经由下转移到上面的接口和协议处了。AHCI和SATA已经不能满足高性能和低延时SSD的需求，因此SSD迫切需要自己更快、更高效的协议和接口。

时势造英雄，在这样的背景下，NVMe横空出世。2009年下半年，在带头大哥Intel的领导下，美光、戴尔、三星、Marvell等巨头，一起制定了专门为SSD服务的NVMe协议，旨在将SSD从老旧的SATA和AHCI中解放出来。

何为NVMe？NVMe即Non-Volatile Memory Express，是非易失性存储器标准，是跑在PCIe接口上的协议标准。NVMe的设计之初就有充分利用了PCIe SSD的低延时以及并行性，还有当代处理器、平台与应用的并行性。相比现在的AHCI标准，NVMe标准可以带来多方面的性能提升。NVMe为SSD而生，但不局限于以闪存为媒介的SSD，它同样可以应用在高性能和低延时的3D XPoint这类新型的介质上。

首款支持NVMe标准的产品是三星XS1715，于2013年7月发布。随后陆续有企业级的NVMe标准SSD推出。2015年Intel 750发布，标志着NVMe标准的产品开始进入消费级市场。如今市面上已经出现很多NVMe SSD产品，包括企业级和消费级，如果说前几年NVMe SSD是阳春白雪，现如今已是下里巴人，NVMe SSD已慢慢进入寻常百姓家。

需要指出的是，在移动设备上，NVMe也占有一席之地。苹果自iPhone 6s开始，其存储设备上跑的就是NVMe协议标准。未来移动存储的方向，笔者认为不是UFS，当然更不会是eMMC，而是NVMe，拭目以待吧。

那么，NVMe究竟有什么好？跟AHCI相比，它有哪些优势？

NVMe和AHCI相比，它的优势主要体现在以下几点：

1.低时延（Latency）

造成硬盘存储时延的三大因素：存储介质本身、控制器以及软件接口标准。

- 存储介质层面，闪存（Flash）比传统机械硬盘速度快太多了。

- 控制器方面，从SATA SSD发展成PCIe SSD，原生PCIe主控与CPU直接相连，而不像传统方式，要通过南桥控制器中转再连接CPU，因此基于PCIe的SSD时延更低。

- 软件接口方面，NVMe缩短了CPU到SSD的指令路径，比如NVMe减少了对寄存器的访问次数；使用了MSI-X中断管理；并行&多线程优化——NVMe减少了各个CPU核之间的锁同步操作等。

所以基于PCIe+NVMe的SSD具有非常低的延时，如图6-1所示。

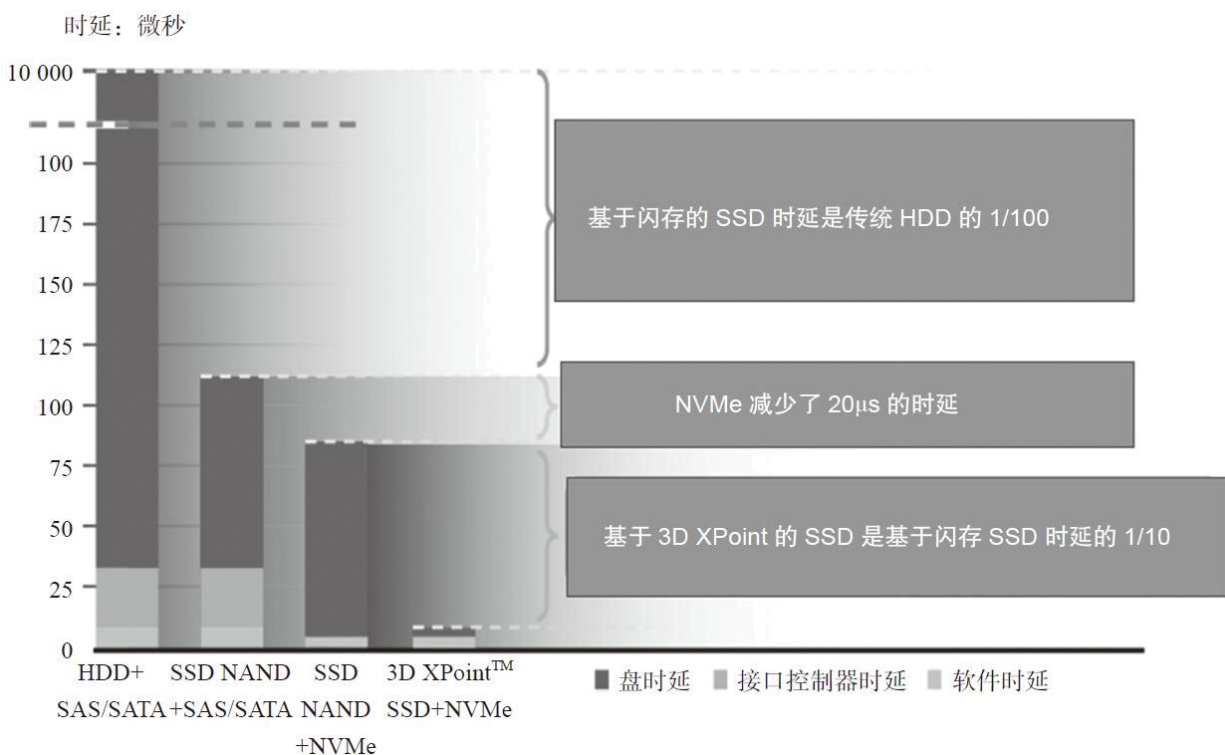


图6-1 时延对比

2.高性能（Throughput&IOPS）

理论上， $IOPS = \text{队列深度} / \text{IO延迟}$ ，故IOPS的性能与队列深度有较大的关系（但IOPS并不与队列深度成正比，因为实际应用中，随着队列深度的增加，IO延迟也会提高）。市面上性能不错的SATA接口SSD，在队列深度上都可以达到32，然而这也是AHCI所能做到的极限。但目前高端的企业级PCIe SSD，其队列深度可能要达到128，甚至是256才能够发挥出最高的IOPS性能。而在NVMe标准下，最大的队列深度可达64K。此外，NVMe的队列数量也从AHCI的1，提高到了64K。

PCIe接口本身在性能上碾压SATA，再加上NVMe具有比AHCI更深、更宽的命令队列，NVMe SSD在性能上秒杀SATA SSD是水到渠成的事情。图6-2是NVMe SSD、SAS SSD和SATA SSD的性能对比图。

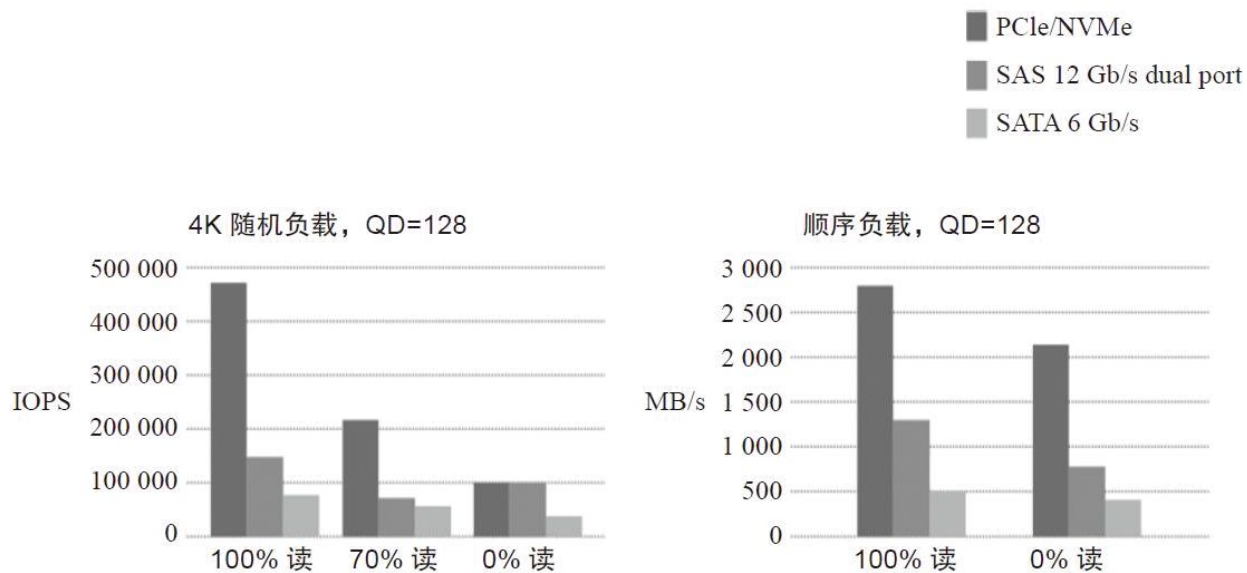


图6-2 NVMe, SAS和SATA SSD性能对比图

3.低功耗

NVMe加入了自动功耗状态切换和动态能耗管理功能，具体在本书的第8章会介绍，这里不再赘述。

下面大部分章节来源于www.ssdfans.com的《蛋蛋读NVMe》系列。另外，最新NVMe协议标准是NVMe1.3，但本章是基于NVMe1.2写的，请读者知晓。

6.2 NVMe综述

NVMe是一种主机（Host）与SSD之间通信的协议，它在协议栈中隶属高层，如图6-3所示。



图6-3 NVMe处于协议栈的最高层

NVMe作为命令层和应用层协议，理论上可以适配在任何接口协议上。但NVMe协议的原配是PCIe，因此如无特别说明，后面章节都是基于NVMe+PCIe。

NVMe在协议栈中处于应用层或者命令层，它是指挥官、军师，相当于三国时期诸葛亮的角色，“运筹帷幄之中，决胜千里之外”。军师设计好计谋，就交由手下五虎大将去执行。NVMe的手下大将就是PCIe，它所制定的任何命令，都交由PCIe去完成。虽然NVMe的命令也可以由别的接口完成，但NVMe与PCIe合作形成的战斗力无疑是最强的。

NVMe是为SSD所生的。NVMe出现之前，SSD绝大多数用的是AHCI加SATA的组合，后者其实是为传统HDD服务的。与HDD相比，SSD具有更低的延时和更高的性能，AHCI已经不能跟上SSD性能发展的步伐，而是成为了制约SSD性能的瓶颈。所有SATA接口的SSD，你

去看性能参数，会发现都不会超过600MB/s（或者说都不超过560MB/s）。

如果碰到有人跟你说他的SATA SSD读取性能可以超过600MB/s，直接拨打12315投诉。不是底层闪存带宽不够，是SATA接口速度限制了带宽，因为SATA 3.0最高带宽就是600MB/s，而且不会再有SATA 4.0了，如图6-4所示。

	SATA		PCIe	
	2.0	3.0	2.0	3.0
链路速度	3Gbps	6Gbps	8Gbps(× 2) 16Gbps(× 4)	16Gbps(× 2) 32Gbps(× 4)
有效数据速率	约 275MB/s	约 560MB/s	约 780MB/s 约 1 560MB/s	约 1 560MB/s 约 3 120MB/s

图6-4 SATA和PCIe接口速度对比

好吧，既然SATA接口速度太慢，那么用PCIe好了，不过上层协议还是AHCI。五虎上将有了，由刘备指挥，让人不禁感叹暴殄天物呀。刘备什么水平，诸葛亮出现之前，居无定所，一会跟着曹操混，一会又跟着吕布混，谁肯收留就跟谁混，惨呀！AHCI和刘备一个德行，只有一个命令队列，最多同时只能发32条命令，HDD时代（群雄逐鹿）还能混混，SSD时代（三足鼎立）就只有被灭的份。刘备需要三顾茅庐，请诸葛亮出山辅佐。同样，SSD需要PCIe，更需要NVMe。

在这样的背景下，Intel等巨头携天子以令诸侯，集大家的智慧，制定出了NVMe规范，目的就是释放SSD性能潜力，解SSD倒悬之苦。最初制定NVMe规范的主要公司如图6-5所示。



图6-5 最初制定NVMe规范的主要公司

NVMe制定了主机与SSD之间通信的命令，以及命令如何执行的。NVMe有两种命令，一种叫Admin命令，用以主机管理和控制SSD；另外一种就是I/O命令，用以主机和SSD之间数据的传输，如图6-6所示。

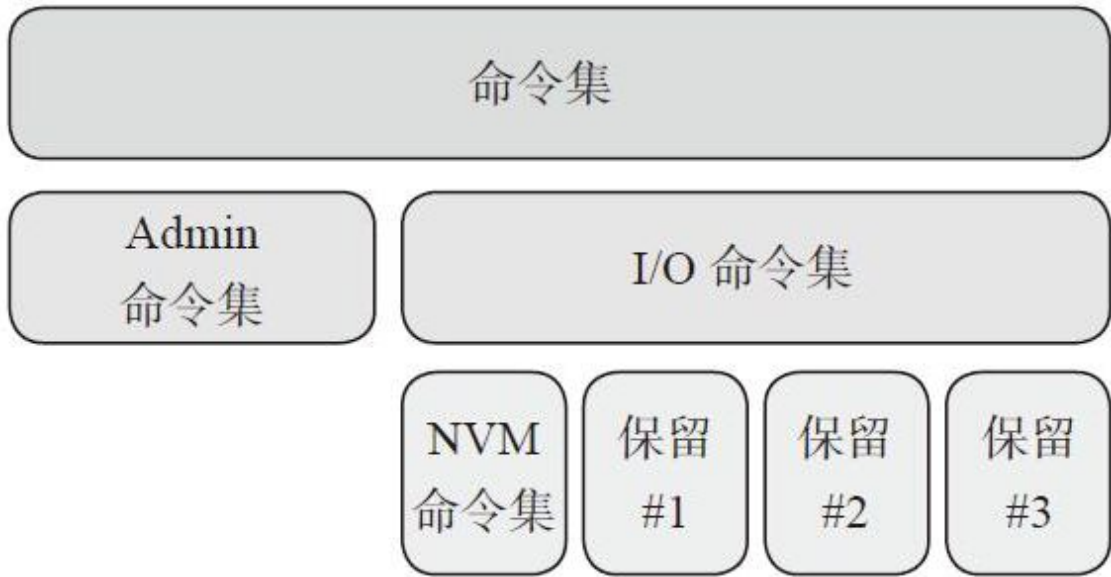


图6-6 NVMe命令集

NVMe支持的Admin命令如图6-7所示。

命令	必须还是可选	种类
Create I/O Submission Queue	必须	Queue 管理
Delete I/O Submission Queue	必须	
Create I/O Completion Queue	必须	
Delete I/O Completion Queue	必须	
Identify	必须	配置
Get Features	必须	
Set Features	必须	
Get Log Page	必须	汇报状态信息
Asynchronous Event Request	必须	
Abort	必须	中止命令
Firmware Image Download	可选	固件更新 / 管理
Firmware Activate	可选	
I/O Command Set Specific Commands	可选	I/O 命令集特有
Vendor Specific Commands	可选	商家特有

图6-7 NVMeAdmin命令集

命令	必须还是可选	种类
Read	必须	必须的数据命令
Write	必须	
Flush	必须	
Write Uncorrectable	可选	可选的数据命令
Write Zeros	可选	
Compare	可选	
Dataset Management	可选	数据暗示
Reservation Acquire	可选	Reservation 命令
Reservation Register	可选	
Reservation Release	可选	
Reservation Report	可选	
Vendor Specific Commands	可选	商家特有

图6-8 NVMe NVM命令集

跟ATA规范中定义的命令相比，NVMe的命令个数少了很多，完全是为SSD量身定制的。在SATA时代，即使只有HDD才需要的命令（SSD上其实完全没有必要），但为了符合协议标准，SSD还是需要实现那些毫无意义（完全只是为了兼容性）的命令。没有办法，谁叫你SSD寄人篱下呢。NVMe让SSD扬眉吐气了一把。

大家现在别纠结于具体的命令，了解一下就好。本章旨在授之以“渔”，而非“鱼”，因此不会介绍具体的NVMe命令，不会把协议命令搬过来凑篇幅。

命令有了，那么，主机又是怎么把这些命令发送给SSD执行呢？

NVMe有三宝：Submission Queue（SQ）、Completion Queue（CQ）和Doorbell Register（DB）。SQ和CQ位于主机的内存中，DB则位于SSD的控制器内部，如图6-9所示。

这张图信息量比较大，除了让我们知道SQ和CQ在主机内存（Memory）中以及DB在SSD端外，而且让我们对一个PCIe系统有一个直观的认识。图6-9中的NVMe子系统一般就是SSD。请看这张图几秒钟，然后闭上眼，脑补SSD所处的位置：SSD作为一个PCIe Endpoint（EP）通过PCIe连着Root Complex（RC），然后RC连接着CPU和内存。RC是什么？我们可以认为RC就是CPU的代言人或者助理。作为系统中的最高层，CPU说：“我很忙的，你SSD有什么事情先跟我助理说！”尽管如此，SSD的地位还是较过去提升了一级，过去SSD别说直接接触霸道总裁，就是连助理的面都见不到，SSD和助理之间还隔着一座南桥。

回到我们的“吉祥三宝”（SQ、CQ、DB）。SQ位于主机内存中，主机要发送命令时，先把准备好的命令放在SQ中，然后通知SSD来取；CQ也是位于主机内存中，一个命令执行完成，成功或失败，SSD总会往CQ中写入命令完成状态。DB（大宝）又是干什么用的呢？主机发送命令时，不是直接往SSD中发送命令，而是把命令准备好放在自己的内存中，那怎么通知SSD来获取命令执行呢？主机就是通过写SSD端的大宝寄存器来告知SSD的。

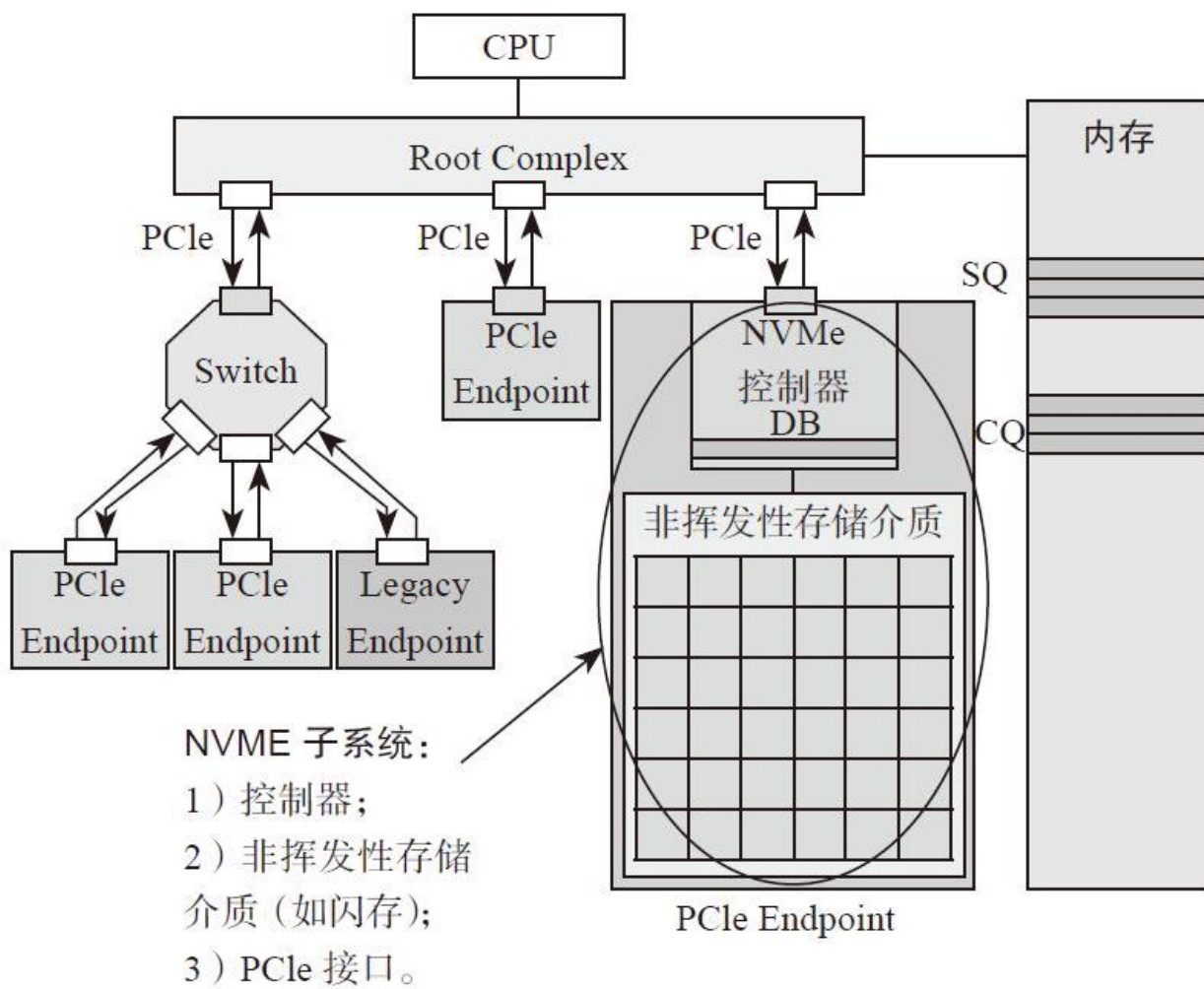


图6-9 SQ、CQ和DB在系统中的位置

我们来看看NVMe是如何处理命令的，如图6-10所示。

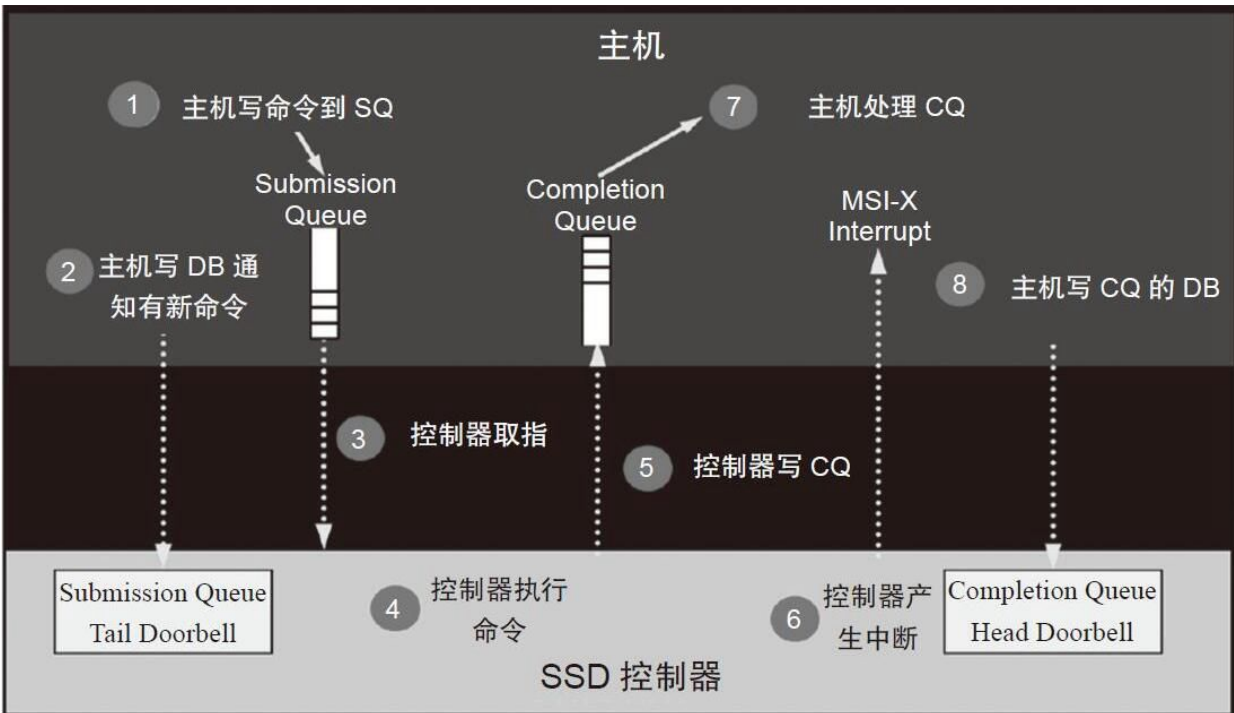


图6-10 NVMe命令处理流程

说，把大象放冰箱一共要几步？

答：三步。

第一步，打开冰箱门；

第二步，放进大象；

第三步，关上冰箱门。

说，NVMe处理命令需要几步？ 答：八步。

第一步，主机写命令到SQ；

第二步，主机写SQ的DB，通知SSD取指；

第三步，SSD收到通知后，到SQ中取指；

第四步，SSD执行指令；

第五步，指令执行完成，SSD往CQ中写指令执行结果；

第六步，然后SSD发中断通知主机指令完成；

第七步，收到中断，主机处理CQ，查看指令完成状态；

第八步，主机处理完CQ中的指令执行结果，通过DB回复SSD：指令执行结果已处理，辛苦您了！

6.3 吉祥三宝：SQ、CQ和DB

接下来我们来详细看看NVMe的吉祥三宝。

主机往SQ中写入命令，SSD往CQ中写入命令完成结果。SQ与CQ的关系，可以是一对一的关系，也可以是多对一的关系，但不管怎样，它们是成对的：有因就有果，有SQ就必然有CQ。

有两种SQ和CQ，一种是Admin，另外一种是IO，前者放Admin命令，用以主机管理控制SSD，后者放置IO命令，用以主机与SSD之间传输数据。Admin SQ/CQ和IO SQ/CQ各司其职，你不能把Admin命令放到IO SQ中，同样，你也不能把IO命令放到Admin SQ里面。IO SQ/CQ不是一生下来就有的，它们是通过Admin命令创建的。

正如图6-11所示，系统中只有1对Admin SQ/CQ，它们是一一对应的关系；IO SQ/CQ却可以有很多，多达65535对（64K减去1对Admin SQ/CQ）。

需要指出的是，对NVMe over Fabrics，SQ和CQ的关系只能是一对一；IO SQ/CQ也不是通过Admin命令创建的。

主机端每个CPU核（Core）可以有一个或者多个SQ，但只有一个CQ。给每个CPU核分配一对SQ/CQ好理解，为什么一个CPU核中还要多个SQ呢？一是性能需求，一个CPU核中有多线程，可以做到一个线程独享一个SQ；二是QoS需求，什么是QoS？Quality of Service，服务质量。脑补一个场景，蛋蛋一边看小电影，同时在后台用迅雷下载小电影，由于电脑配置差，看个小电影都卡。蛋蛋不要卡顿！怎么办？NVMe建议，你设置两个SQ，一个赋予高优先级，一个低优先级，把看小电影所需的命令放到高优先级的SQ，迅雷下载所需的命令放到低优先级的SQ，这样，你的电脑就能把有限的资源优先满足你看小电影了。至于迅雷卡不卡，下载慢不慢，这个时候已经不重要了。能让蛋蛋舒舒服服地看完一部小电影，就是好的QoS。实际系统中用多少个SQ，取决于系统配置和性能需求，可灵活设置I/O SQ个数。

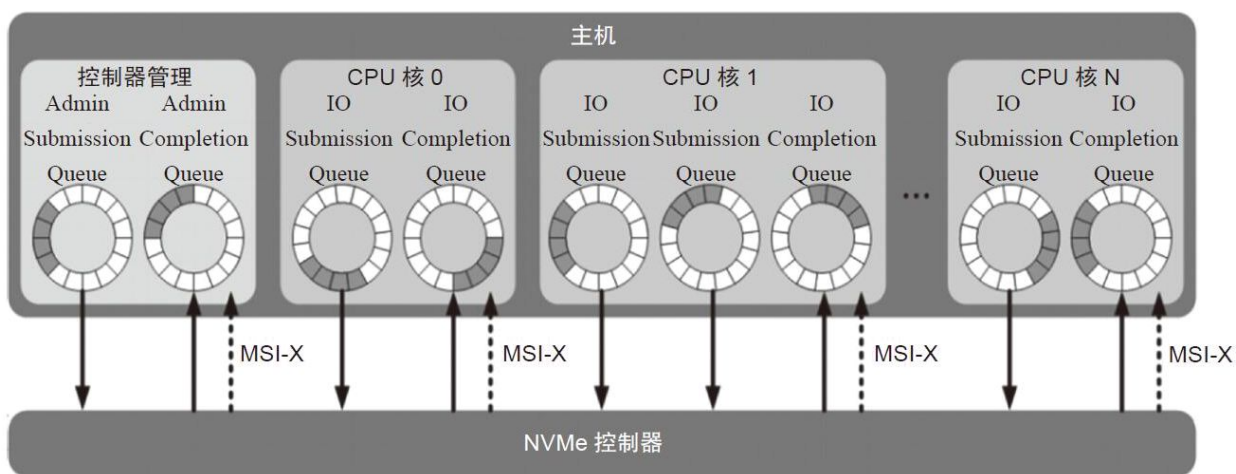


图6-11 SQ和CQ

关于系统中IO SQ的个数，NVMe白皮书给出如下建议（见表6-1）。

表6-1 NVMe白皮书对NVMe的配置建议

特性	企业级应用推荐	消费级应用推荐
IO 队列数	16 到 128	2 到 8
物理不连续队列	取决于设计	不要
逻辑块大小	4KB	4KB
中断支持	MSI-X	MSI-X
固件更新	支持	支持
端到端数据保护	支持	不支持
SR-IOV 支持	支持	不支持

作为队列，每个SQ和CQ都有一定的深度：对Admin SQ/CQ来说，其深度可以是2~4096（4K）；对IO SQ/CQ，深度可以是2~65536（64K）。队列深度也是可以配置的。

SQ/CQ的个数可以配置，每个SQ/CQ的深度也可以配置，因此NVMe的性能是可以通过配置队列个数和队列深度来灵活调节的。

百变星君NVMe：想胖就胖，想瘦就瘦；想高就高，想矮就矮。

我们已经知道，AHCI只有一个命令队列，且队列深度是固定的32，和NVMe相比，无论是在命令队列广度还是深度上，都是无法望其项背的；NVMe命令队列的百般变化，更是AHCI无法做到的。说到百

般变化，我突然又想到一件残忍的事情：PCIe也是可以的。一个PCIe接口，可以有1、2、4、8、12、16、32条lane！SATA都要哭了：单挑都挑不过你，你还来群殴我，太欺负人了。

每个SQ放入的是命令条目，无论是Admin还是IO命令，每个命令条目大小都是64字节；每个CQ放入的是命令完成状态信息条目，每个条目大小是16字节。

在继续谈大宝（DB）之前，先对SQ和CQ做个小结：

- SQ用以主机发命令，CQ用以SSD回命令完成状态；
- SQ/CQ可以在主机的内存中，也可以在SSD中，但一般在主机内存中（本书中除非特殊说明，不然都是基于SQ/CQ在主机内存中作介绍）；
- 两种类型的SQ/CQ：Admin和IO，前者发送Admin命令，后者发送IO命令；
- 系统中只能有一对Admin SQ/CQ，但可以有很多对IO SQ/CQ；
- IO SQ与CQ可以是一对一的关系，也可以是多对一的关系；
- IO SQ是可以赋予不同优先级的；
- IO SQ/CQ深度可达64K，Admin SQ/CQ深度可达4K；
- IO SQ/CQ的广度和深度都可以灵活配置；
- 每条命令大小是64B，每条命令完成状态是16B。

SQ/CQ中的“Q”指Queue，队列的意思（见图6-12），无论SQ还是CQ，都是队列，并且是环形队列。队列有几个要素，除了队列深度、队列内容，还有队列的头部（Head）和尾部（Tail）。

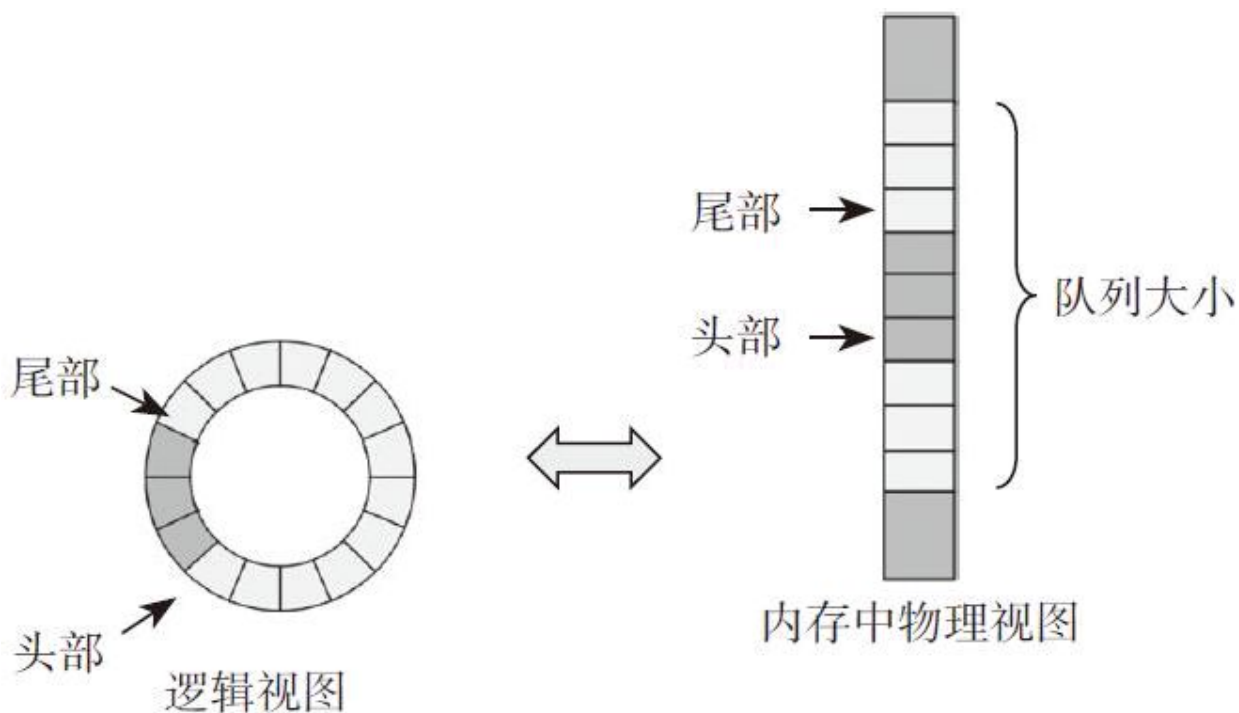


图6-12 队列（Queue）的概念

队伍头部的那个正在被服务或者等待被服务，一旦完成，就离开队伍。可见队列的头尾很重要，头决定谁会被马上服务，尾巴决定了新来的人站的位置。**DB**就是用来记录了一个**SQ**或者**CQ**的头和尾。每个**SQ**或者**CQ**，都有两个对应的**DB**：**Head DB**和**Tail DB**。**DB**是在**SSD**端的寄存器，记录**SQ**和**CQ**的头和尾巴的位置。

如图6-13所示是一个队列生产者/消费者（**Producer/Consumer**）模型。生产者往队列的尾部写入东西，消费者从队列的头部取出东西。对一个**SQ**来说，它的生产者是主机，因为它向**SQ**的尾部写入命令，消费者是**SSD**，因为它从**SQ**的头部取出指令执行；对一个**CQ**来说，刚好相反，生产者是**SSD**，因为它向**CQ**的尾部写入命令完成信息，消费者则是主机，它从**CQ**的头部取出命令完成信息。

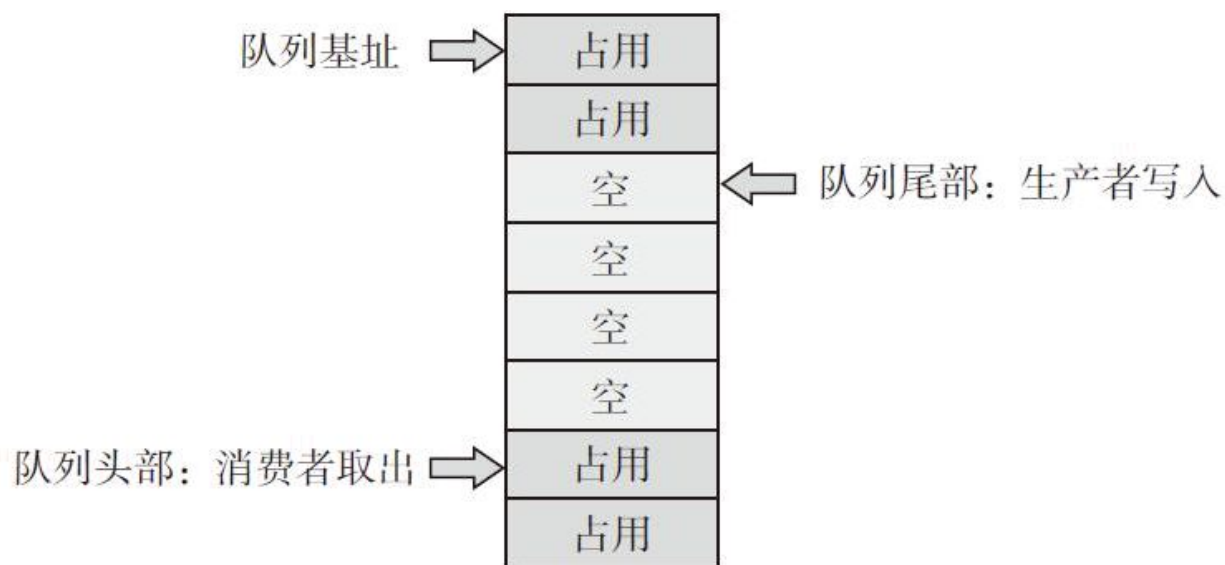


图6-13 队列生产者/消费者模型

下面举个例子说明。

1) 开始假设SQ1和CQ1是空的，Head=Tail=0，如图6-14所示。

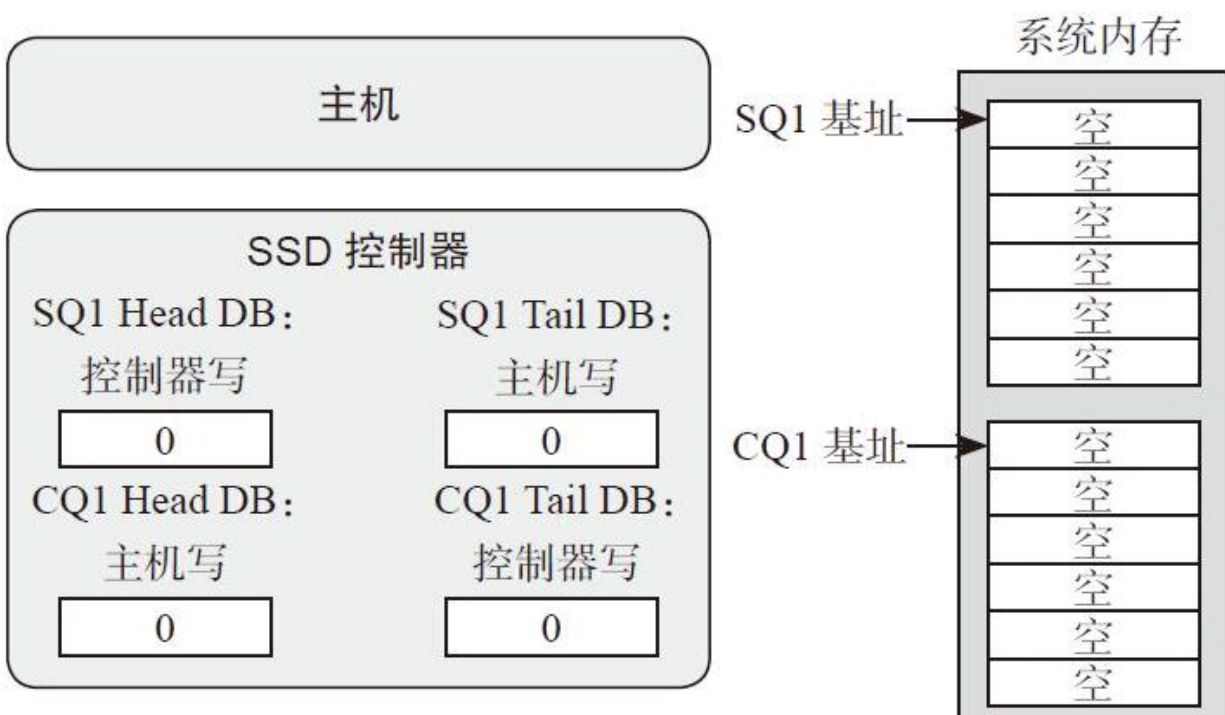


图6-14 SQ、CQ、DB初始化状态

- 2) 这个时候，主机往SQ1中写入了三个命令，SQ1的Tail则变成3。主机往SQ1写入三个命令后，然后漂洋过海去更新SSD控制器端的SQ1Tail DB寄存器，值为3。主机更新这个寄存器的同时，也是在告诉SSD控制器：有新命令了，帮忙去我那里取一下，如图6-15所示。
- 3) SSD控制器收到通知后，于是派人去SQ1把3个命令都取回来执行。SSD把SQ1的三个命令都消费了，SQ1的Head从而也调整为3，SSD控制器会把这个Head值写入本地的SQ1Head DB寄存器，如图6-16所示。
- 4) SSD执行完了两个命令，于是往CQ1中写入两个命令完成信息，更新CQ1对应的Tail DB寄存器，值为2。同时发消息给主机：有命令完成，请注意查看，如图6-17所示。

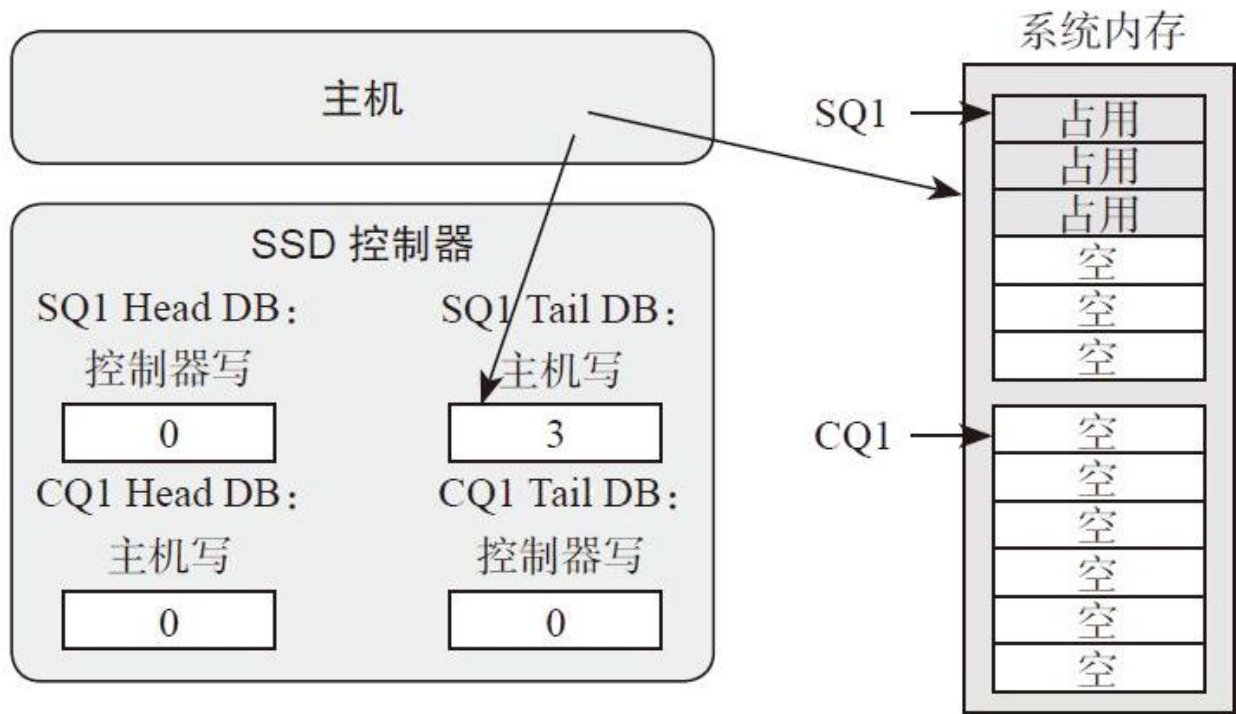


图6-15 主机往SQ中写入三个命令

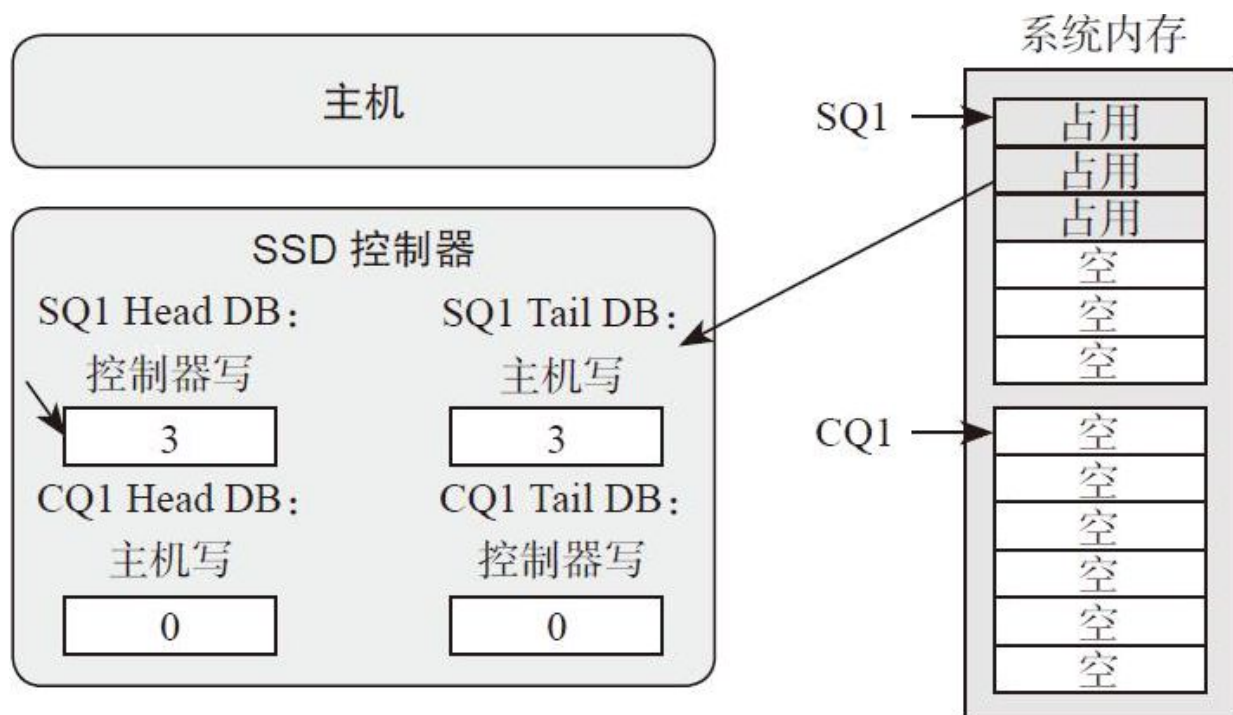


图6-16 SSD取走三个命令

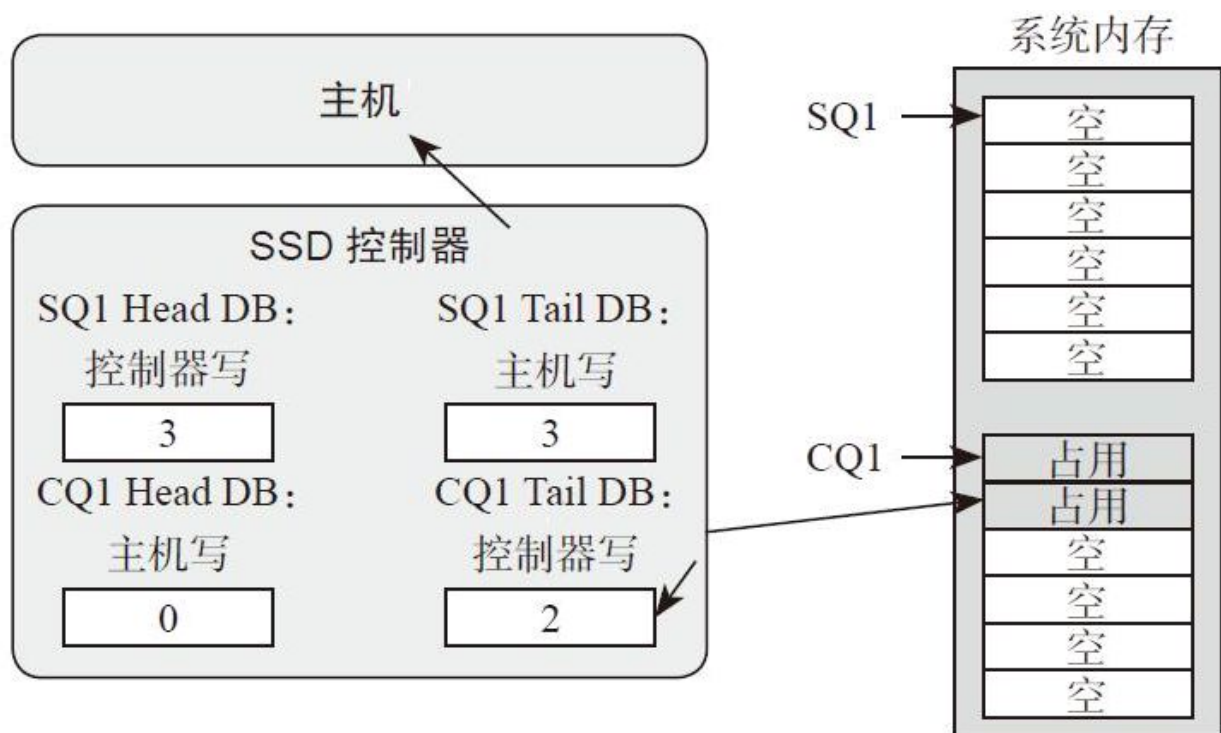


图6-17 SSD完成两个命令后写CQ

5) 主机收到SSD的短信通知（中断信息），于是从CQ1中取出那两条完成信息。处理完毕，主机又漂洋过海地往CQ1Head DB寄存器中写入CQ1的head，值为2，如图6-18所示。

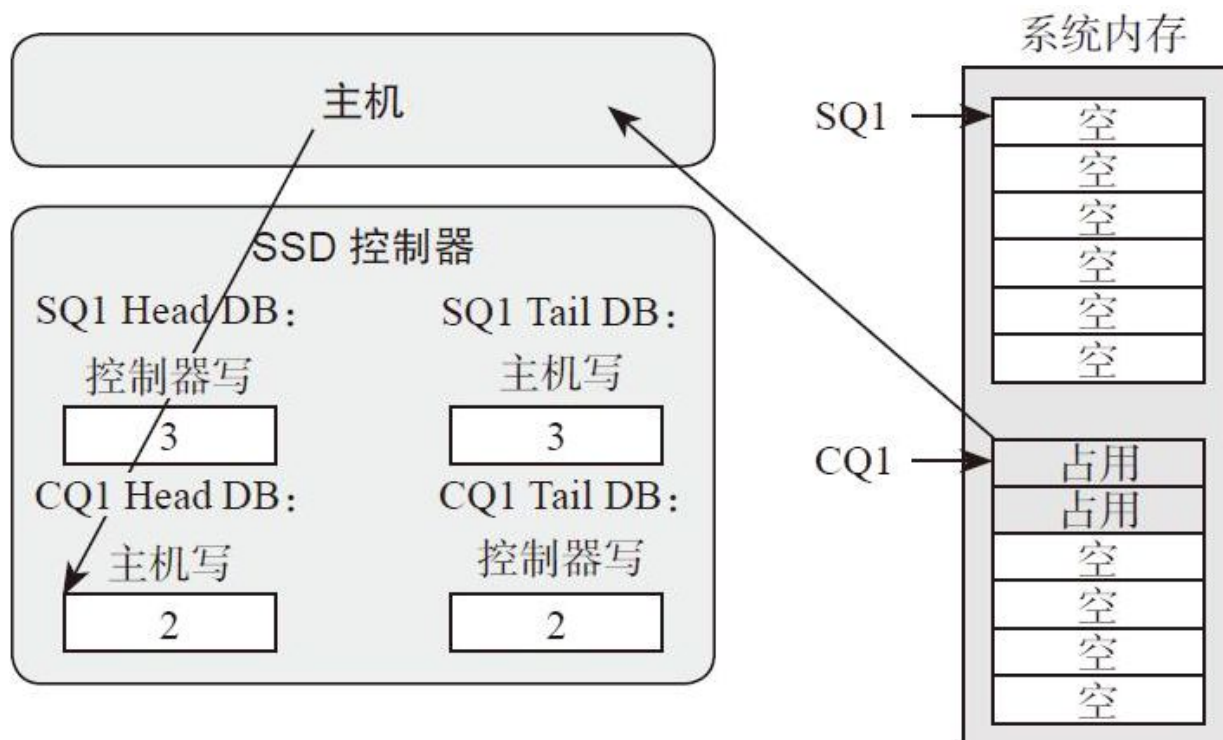


图6-18 主机处理完CQ中的两个命令状态

通过这个例子，我们又重温了一下命令处理流程。之前也许只记住了命令处理需要8步（距离曹植一步之遥），但现在我们应该对命令处理流程有了更深入具体的认识。

那么，DB在命令处理流程中起了什么作用呢？

首先，如前文提到的，它记住了SQ和CQ的头和尾。对SQ来说，SSD是消费者，它直接和队列的头打交道，很清楚SQ的头在哪里，所以SQ head DB由SSD自己维护；但它不知道队伍有多长，尾巴在哪，后面还有多少命令等待执行，相反，主机知道，所以SQ Tail DB由主机来更新。SSD结合SQ的头和尾，就知道还有多少命令在SQ中等待执行了。对CQ来说，SSD是生产者，它很清楚CQ的尾巴在哪里，所以CQ Tail DB由自己更新，但是SSD不知道主机处理了多少条命令完成信息，需要主机告知，因此CQ Head DB由主机更新。SSD根据CQ的头和尾，就知道CQ还能不能，以及能接受多少命令完成信息。

DB还起到了通知作用：主机更新SQ Tail DB的同时，也是在告知SSD有新的命令需要处理；主机更新CQ Head DB的同时，也是在告知SSD，你返回的命令完成状态信息我已经处理，同时表示谢意。

这里有一个对主机不公平的地方，主机对DB只能写（还仅限于写SQ Tail DB和CQ Head DB），不能读取DB。

在这个限制下，我们看看主机是怎样维护SQ和CQ的。SQ的尾巴没有问题，主机是生产者，对新命令来说，它清楚自己应该站在队伍哪里。但是Head呢？SSD在取指的时候，是偷偷进行的，主机对此毫不知情。主机发了取指通知后，它并不清楚SSD什么时候去取命令、取了多少命令。怎么办？机智如你，如果是你，你会怎么做？山人自有妙计。给个提示（见图6-19）。



图6-19 SQ的Head DB在命令完成状态里

这是什么？这是SSD往CQ中写入的命令完成状态信息（16字节）。

是的，SSD往CQ中写入命令状态信息的同时，还把SQ Head DB的信息告知了主机！这样，主机对SQ队列的头部和尾部的信息就都有了，可以轻松玩转SQ。

CQ呢？主机知道它队列的头部，不知道尾部。那怎么能知道尾部呢？思路很简单，既然SSD知道，那你告诉我呗！SSD怎么告诉主机

呢？还是通过SSD返回命令状态信息获取。看到图6-19中所示的“P”了吗？干什么用？做标记用。

具体是这样的：一开始CQ中每条命令完成将条目中的“P”比特初始化为0的工作，SSD在往CQ中写入命令完成条目时，会把“P”写成1（如果之前该位置为1，控制器写CQ的时候翻转该比特，即写0）。记住一点，CQ是在主机端的内存中，主机可以检查CQ中的所有内容，当然包括“P”了。主机记住上次队列的尾部，然后往下一个一个检查“P”，就能得出新的队列尾部了。就是这样，如图6-20所示。

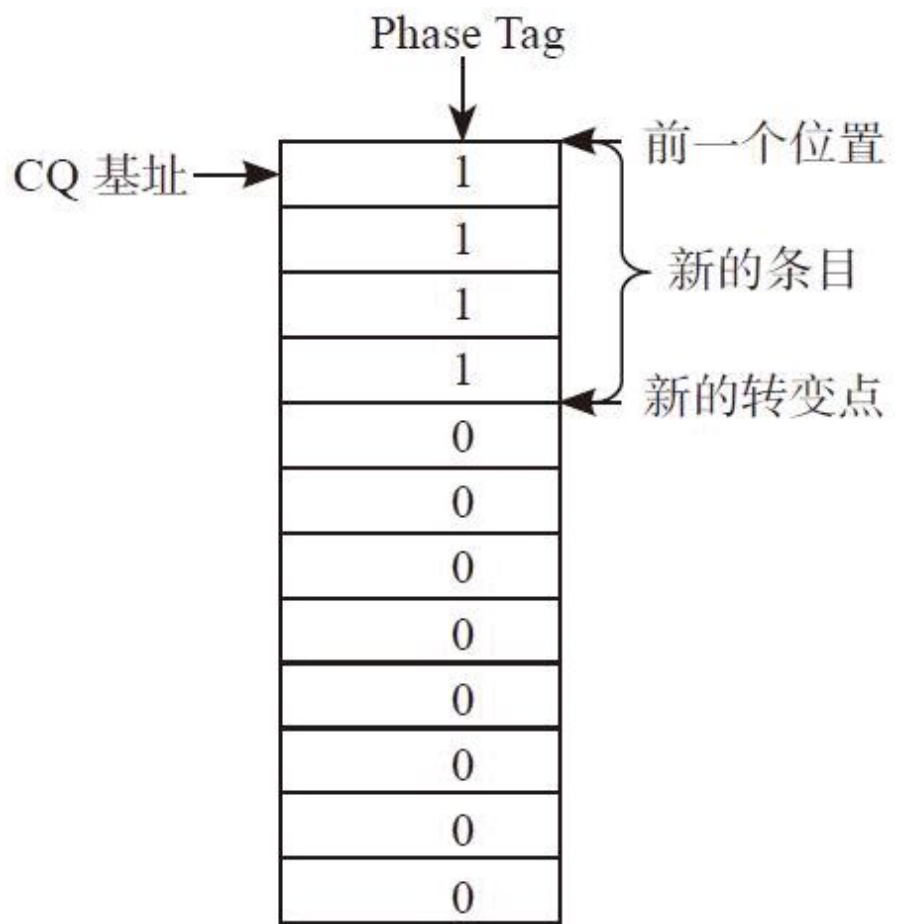


图6-20 主机根据PhaseTag计算CQ队列的尾部

最后，给大宝做个小结：

- DB在SSD控制器端，是寄存器；
- DB记录着SQ和CQ队列的头部和尾部；

- 每个SQ或者CQ有两个DB——Head DB和Tail DB;
- 主机只能写DB, 不能读DB;
- 主机通过SSD往CQ中写入的命令完成状态获取其队列头部或者尾部。

6.4 寻址双雄：PRP和SGL

有个人一直在思考三个问题：我是谁？我从哪里来？我要去哪里？

你猜这个人最后怎么着？

成了哲学家？

疯了？

疯了的哲学家？

我觉得无外乎这三种结果了。

相比人的世界，这三个问题在NVMe的世界就很容易得到答案了，至少不会把人逼疯。

我是数据，我从主机端来，要到SSD去。或者，我是数据，我从SSD来，要去主机端。

主机如果想往SSD上写入用户数据，需要告诉SSD写入什么数据，写入多少数据，以及数据源在内存中的什么位置，这些信息包含在主机向SSD发送的Write命令中。每笔用户数据对应着一个叫作LBA

（Logical Block Address）的东西，Write命令通过指定LBA来告诉SSD写入的是什么数据。对NVMe/PCIe来说，SSD收到Write命令后，通过PCIe去主机的内存数据所在位置读取数据，然后把这些数据写入闪存中，同时生成LBA与闪存位置的映射关系。

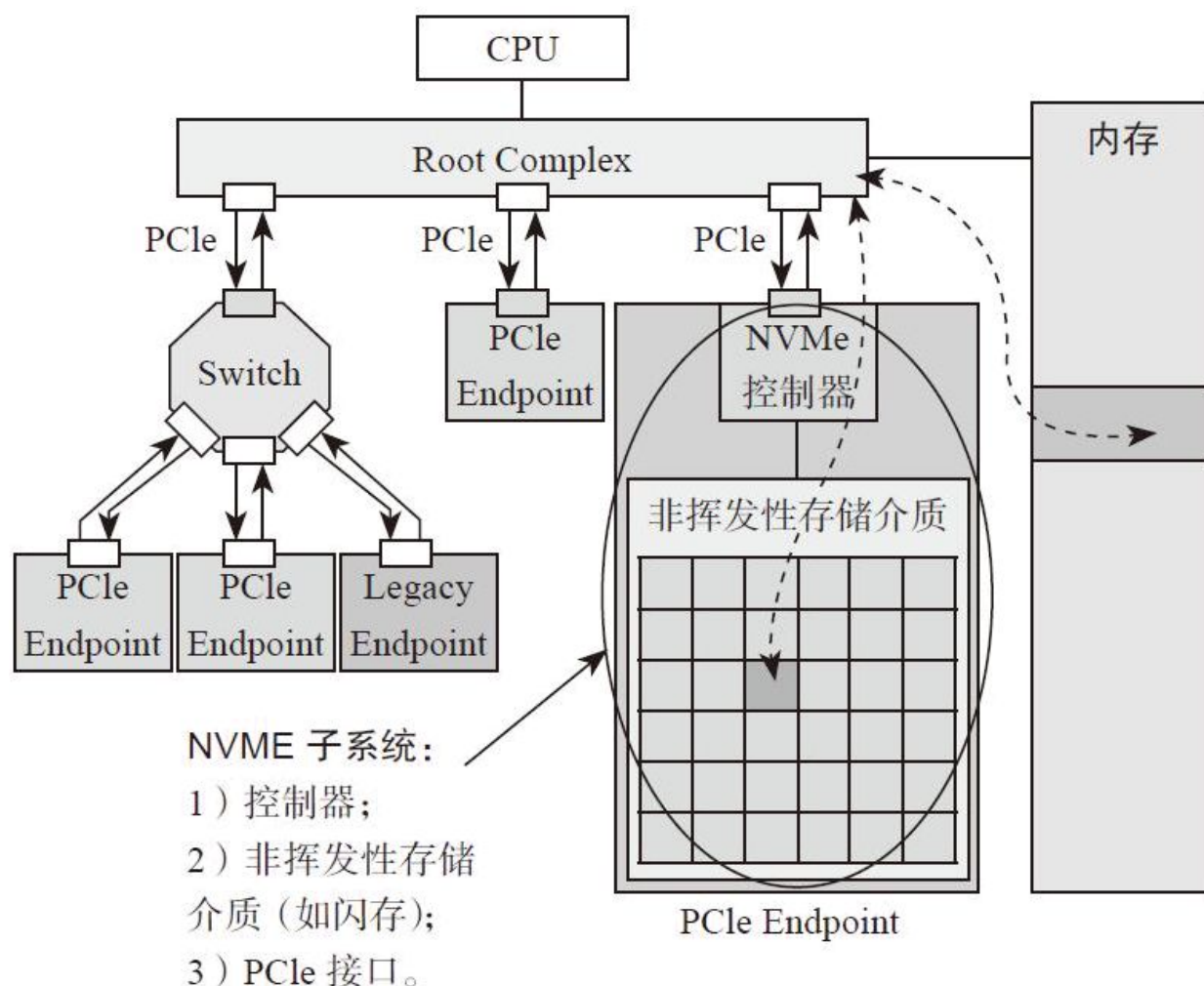


图6-21 数据在主机内存和SSD中流动

主机如果想读取SSD上的用户数据，同样需要告诉SSD需要什么数据，需要多少数据，以及数据最后需要放到主机内存的哪个位置上去，这些信息包含在主机向SSD发送的Read命令中。SSD根据LBA，查找映射表（写入时生成的），找到对应闪存物理位置，然后读取闪存获得数据。数据从闪存读上来以后，对NVMe/PCIe来说，SSD会通过PCIe把数据写入主机指定的内存中。这样就完成了主机对SSD的读访问。

在上面的描述中，大家有没有注意到一个问题，那就是主机在与SSD的数据传输过程中，主机是被动的一方，SSD是主动的一方。主机需要数据，是SSD主动把数据写入主机的内存中；主机写数据，同样是SSD主动去主机的内存中取数据，然后写入闪存。正如快递小哥一样辛劳，SSD不仅送货上门，还上门取件。

无论送货上门，还是上门取件，你都需要告诉快递小哥你的地址，世界那么大，快递小哥怎么就能找到你呢？同样的，主机你不亲自传输数据，那总该告诉我SSD去你内存中什么地方取用户数据，或者要把数据写入到你内存中的什么位置。你在告诉快递小哥送货地址或者取件地址时，会说××路××号××弄××楼××室，也可能会说××小区××楼××室，不管哪种方式，快递小哥能找到就行。主机也有两种方式来告诉SSD数据所在的内存位置，一是PRP（Physical Region Page，物理区域页，有人戏称其为“拼人品”），二是SGL（Scatter/Gather List，分散/聚集列表，有人戏称其为“死过来，送过来”）。

先说PRP。NVMe把主机端的内存划分为一个一个物理页（Page），页的大小可以是4KB，8KB，16KB，...，128MB。

PRP是什么，长什么样呢如图6-22所示。

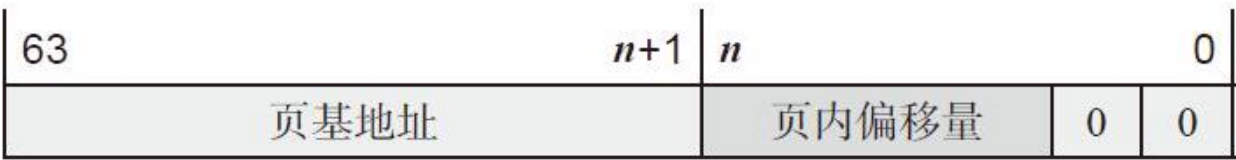


图6-22 PRP条目（Entry）布局（Layout）

PRP Entry本质就是一个64位内存物理地址，只不过把这个物理地址分成两部分：页起始地址和页内偏移。最后两比特是0，说明PRP表示的物理地址只能四字节对齐访问。页内偏移可以是0，也可以是个非零的值，如图6-23所示。

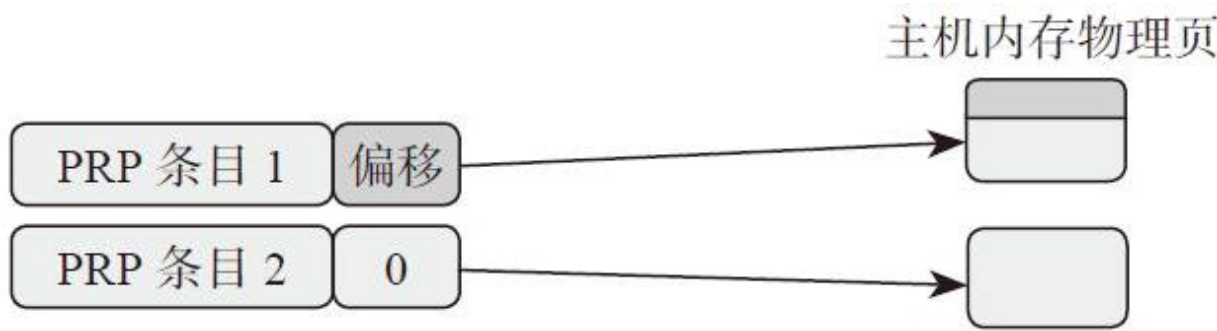


图6-23 PRP描述内存物理空间示例

一个PRP Entry描述的是一个物理页空间。如果需要描述若干个物理页，那就需要若干个PRP Entry。把若干个PRP Entry连接起来，就成了PRP链表（List），如图6-24所示。

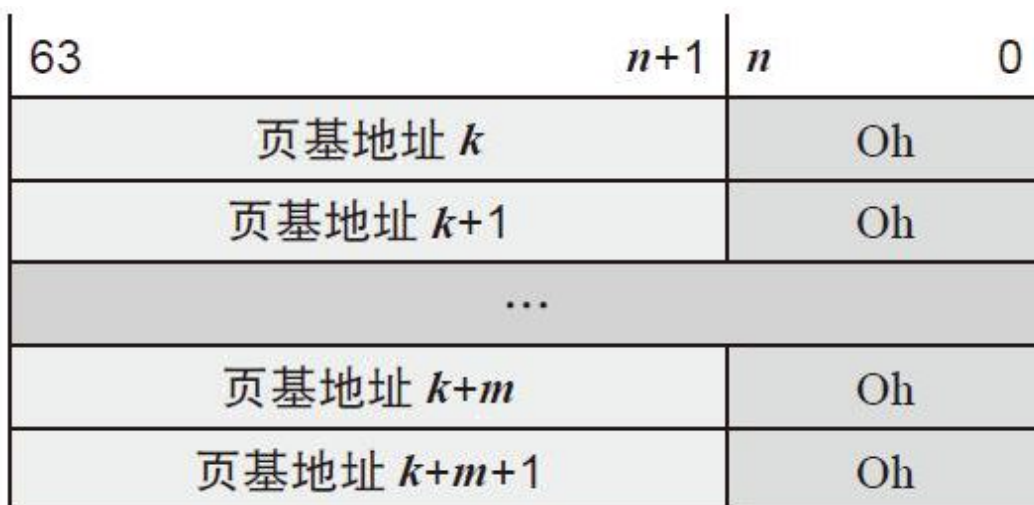


图6-24 PRP链表布局 (Layout)

是的，正如你所见，PRP链表中的每个PRP Entry的偏移量都必须为0，PRP链表中的每个PRP Entry都是描述一个物理页。它们不允许有相同的物理页，不然SSD往同一个物理页写入几次数据，会导致先写入的数据被覆盖。

每个NVMe命令中有两个域：PRP1和PRP2，主机就是通过这两个域告诉SSD数据在内存中的位置或者数据需要写入的地址，如表6-2所示。

表6-2 NVMe命令格式中的PRP

字节	描述
63:60	命令 Dword15 (CDW15): 命令相关
59:56	命令 Dword14 (CDW14): 命令相关
55:52	命令 Dword13 (CDW13): 命令相关
51:48	命令 Dword12 (CDW12): 命令相关

(续)

字节	描述
47:44	命令 Dword11 (CDW11) : 命令相关
43:40	命令 Dword10 (CDW10) : 命令相关
39:32	PRP Entry 2 (PRP2) : 命令中第二个地址条目 (如果有用到的话)
31:24	PRP Entry 1 (PRP1) : 命令中第一个地址条目
23:16	MetadataPointer (MPTR) : 连续元数据缓冲区地址
15:8	保留
7:4	NamespaceIdentifier (NSID)
3:0	命令 Dword0 (CDW0) : 所有命令都用

PRP1和PRP2有可能指向数据所在位置, 也可能指向PRP链表。类似C语言中的指针概念, PRP1和PRP2可能是指针, 也可能是指针的指针, 还有可能是指针的指针的指针。别管你包得有多严实, 根据不同的命令, SSD总能一层一层地剥下包装, 找到数据在内存的真正物理地址。

下面是一个PRP1指向PRP链表的示例, 如图6-25所示。

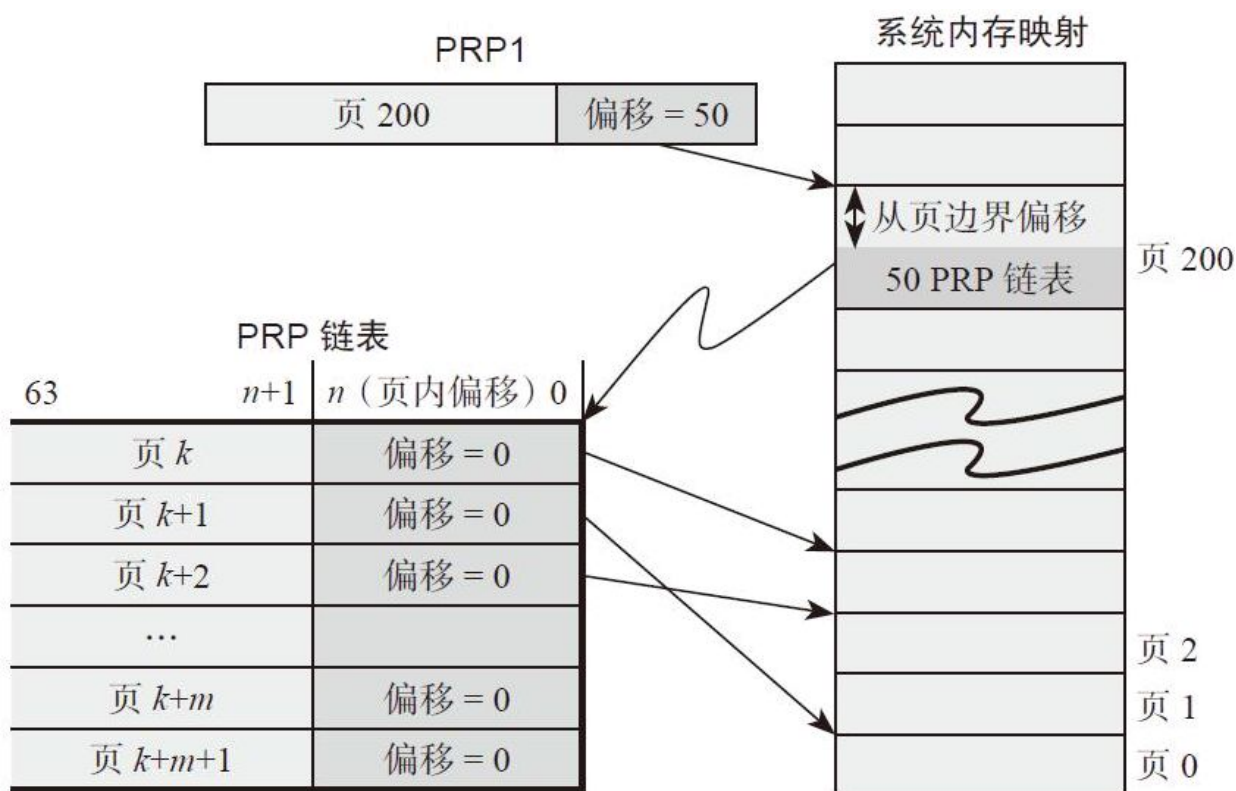


图6-25 PRP链表描述内存空间示例

PRP1指向一个PRP链表，PRP链表位于Page 200，页内偏移50的位置。SSD确定PRP1是个指向PRP链表的指针后，就会去主机内存中（Page 200，Offset 50）把PRP链表取过来。获得PRP链表后，就获得数据的真正物理地址，SSD然后就会向这些物理地址读取或者写入数据。

对Admin命令来说，它只用PRP告诉SSD内存物理地址；对I/O命令来说，除了用PRP，主机还可以用SGL的方式来告诉SSD数据在内存中写入或者读取的物理地址，如表6-3所示。

表6-3 NVMe命令格式中的SGL

字节	描述
63:60	命令 Dword15 (CDW15): 命令相关
59:56	命令 Dword14 (CDW14): 命令相关
55:52	命令 Dword13 (CDW13): 命令相关
51:48	命令 Dword12 (CDW12): 命令相关
47:44	命令 Dword11 (CDW11): 命令相关
43:40	命令 Dword10 (CDW10): 命令相关
39:24	如果 CDW0[15:14]=00b, 这个域解释为 PRP2+PRP1, 即用 PRP 方式描述内存地址; 如果 CDW0[15:14]=01b 或者 10b, 这个域解释为 SGL, 即用 SGL 方式描述内存地址
23:16	MetadataPointer (MPTR): 连续元数据缓冲区地址
15:8	保留
7:4	NamespaceIdentifier (NSID)
3:0	命令 Dword0 (CDW0): 所有命令都用

主机在命令中会告诉SSD采用何种方式。具体来说，如果命令当中DW0[15: 14]是0，就是PRP的方式，否则就是SGL的方式。

SGL是什么？SGL是一个数据结构，用以描述一段数据空间，这个空间可以是数据源所在的空间，也可以是数据目标空间。SGL（Scatter Gather List）首先是个List，是个链表，由一个或者多个SGL段（Segment）组成，而每个SGL段又由一个或者多个SGL描述符（Descriptor）组成。SGL描述符是SGL最基本的单元，它描述了一段连续的物理内存空间：起始地址+空间大小。

每个SGL描述符大小是16字节。一块内存空间，可以用来放用户数据，也可以用来放SGL段，根据这段空间的不同用途，SGL描述符也分几种类型，如表6-4所示。

表6-4 SGL描述符类型

编码	描述符	编码	描述符
0h	SGL 数据块描述符 (Data Block Descriptor)	3h	SGL 末段描述符 (Last Segment Descriptor)
1h	SGL 位桶描述符 (Bit Bucket Descriptor)	4h ~ Eh	保留
2h	SGL 段描述符 (Segment Descriptor)	Fh	商家指定

由表6-4可知，有4种SGL描述符：

- 一种是数据块描述符，这个好理解，就是描述的这段空间是用户数据空间。

- 一种是段描述符，SGL不是由SGL段组成的链表吗？既然是链表，前面一个段就需要有个指针指向下一个段，这个指针就是SGL段描述符，它描述的是它下一个段所在的空间。

- 特别地，对链表当中倒数第二个段，它的SGL段描述符我们把它叫作SGL末段描述符。它本质还是SGL段描述符，描述的还是SGL段所在的空间。为什么需要把倒数第二个SGL段描述符单独的定义成一种类型呢？我认为是让SSD在解析SGL的时候，碰到SGL末段描述符，就知道链表快到头了，后面只有一个段了。

- 那么最后，SGL位桶是什么？它只对主机读有用，用以告诉SSD，你往这个内存写入的东西我是不要的。好吧，你既然不要，我也不传了。

说了这么多，可能有点晕，结合图6-26，可能会更明白点。

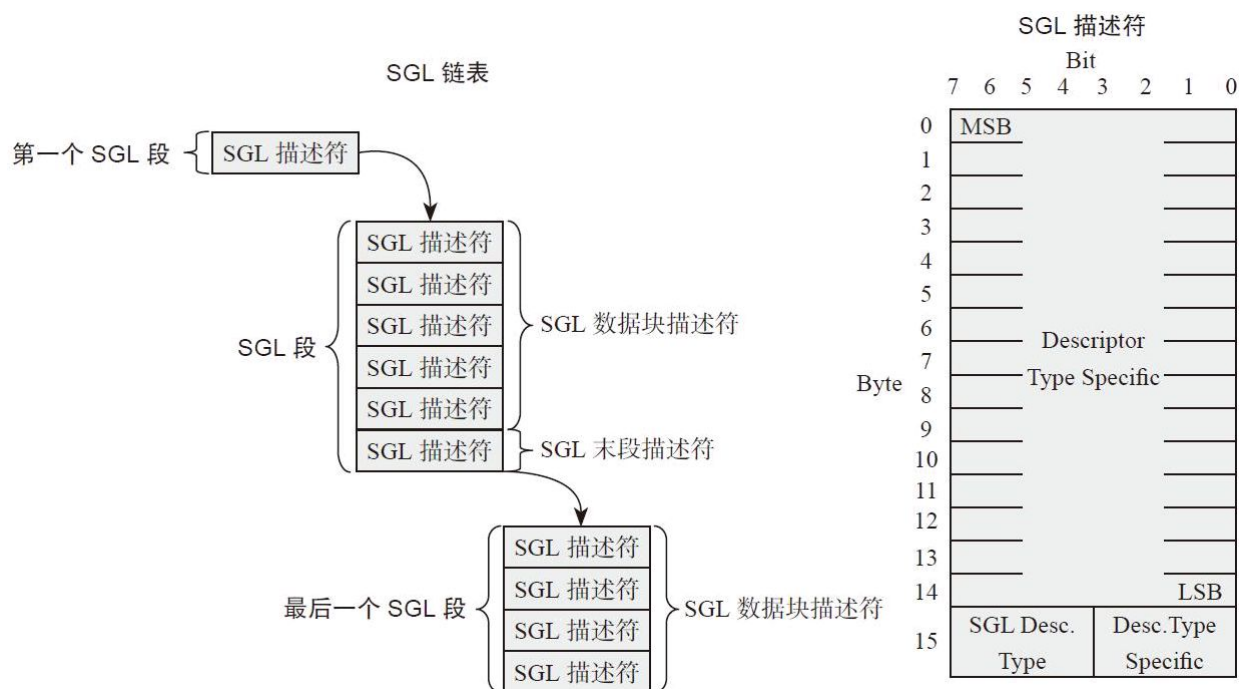


图6-26 SGL示例

如果还是晕，看个例子吧（见图6-27）。

这个例子中，假设主机需要从SSD中读取13KB的数据，其中真正只需要11KB数据，这11KB的数据需要放到3个大小不同的内存中，分别是：3KB、4KB和4KB。

无论是PRP还是SGL，本质都是描述内存中的一段数据空间，这段数据空间在物理上可能是连续的，也可能是不连续的。主机在命令中设置好PRP或者SGL，告诉SSD数据源在内存的什么位置，或者从闪存上读取的数据应该放到内存的什么位置。

大家也许跟我有同样的疑问，那就是，既然有PRP，为什么还需要SGL？事实上，NVMe1.0的时候的确只有PRP，SGL是NVMe1.1之后引入的。那SGL和PRP本质的区别在哪？图6-28道出了真相：PRP描述的是物理页，而SGL可以描述任意大小的内存空间。

对NVMe over PCIe（我们目前讲的都是NVMe跑在PCIe上），Admin命令只支持PRP，I/O命令可以支持PRP或者SGL；对NVMe over Fabrics，所有命令只支持SGL。

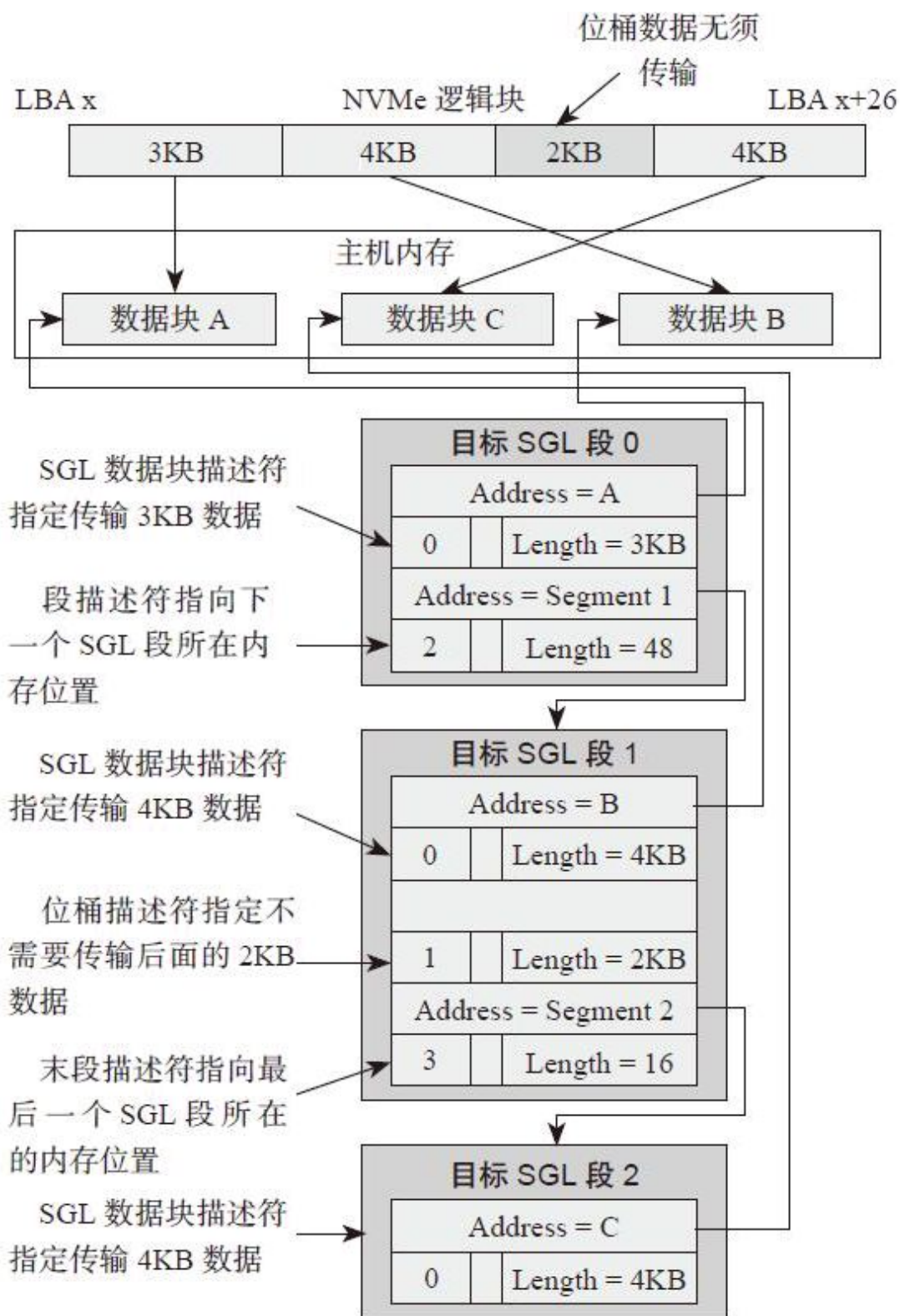


图6-27 SGL读示例

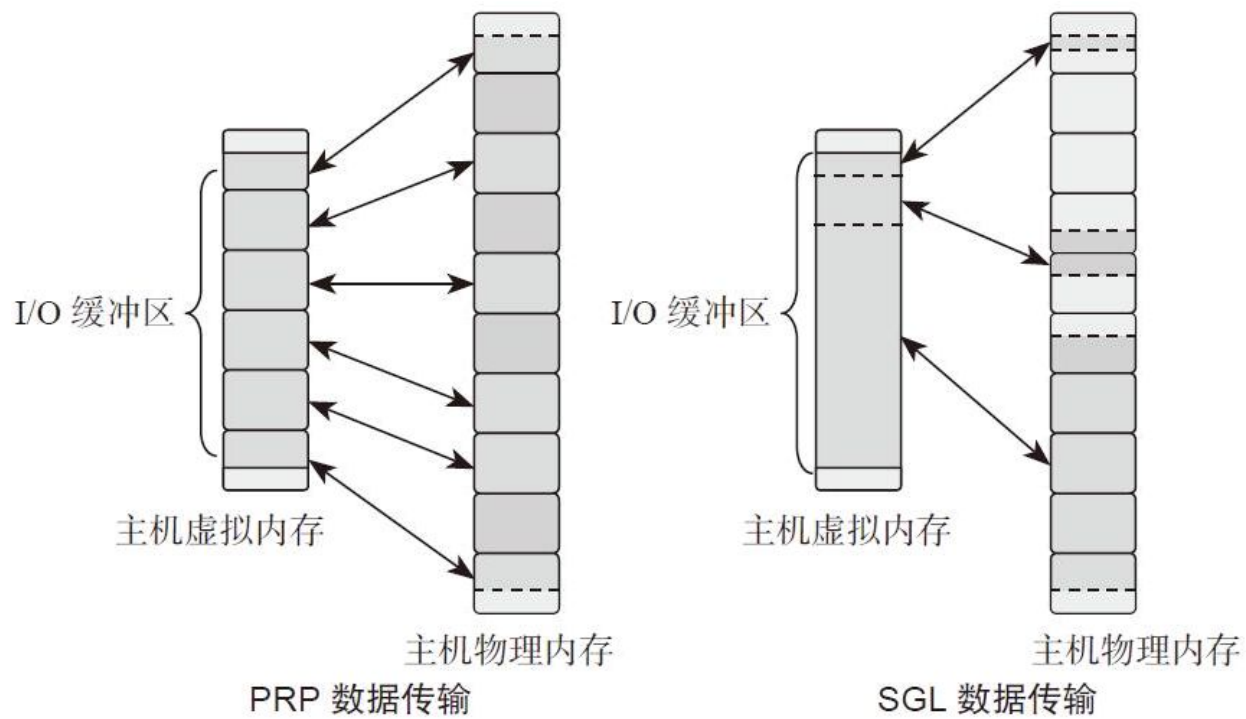


图6-28 PRP vs SGL

6.5 Trace分析

前面我们已经看到过图6-29所示的结构，任何一种计算机协议都是采用这种分层结构的，下层总是为上层服务的。有些协议，图中所有的层次都有定义和实现；而有些协议，只定义了其中的几层。然而，要让一种协议能工作，它需要一个完整的协议栈，PCIe定义了下三层，NVMe定义了最上层，两者一拍即合，构成一个完整的主机与SSD通信的协议。



图6-29 PCIe+NVMe协议栈

PCIe最直接接触的是NVMe的事务层。在NVMe层，我们能看到的是64字节的命令、16字节的命令返回状态，以及跟命令相关的数据。而在PCIe的事务层，我们能看到的是事务层数据包（Transaction Layer Packet），即TLP。还是跟快递做类比，你要寄东西，可能是手机，可能是电脑，不管是什么，你交给快递小哥，他总是把你要寄的东西打包，快递员看到的就是包裹，他根本不关心你里面的内容。PCIe事务层作为NVMe最直接的服务者，不管你NVMe发给我的是命令，还是命令状态，或者是用户数据，我统统帮你放进包裹，打包后交给下一层，即数据链路层继续处理，如图6-30所示。

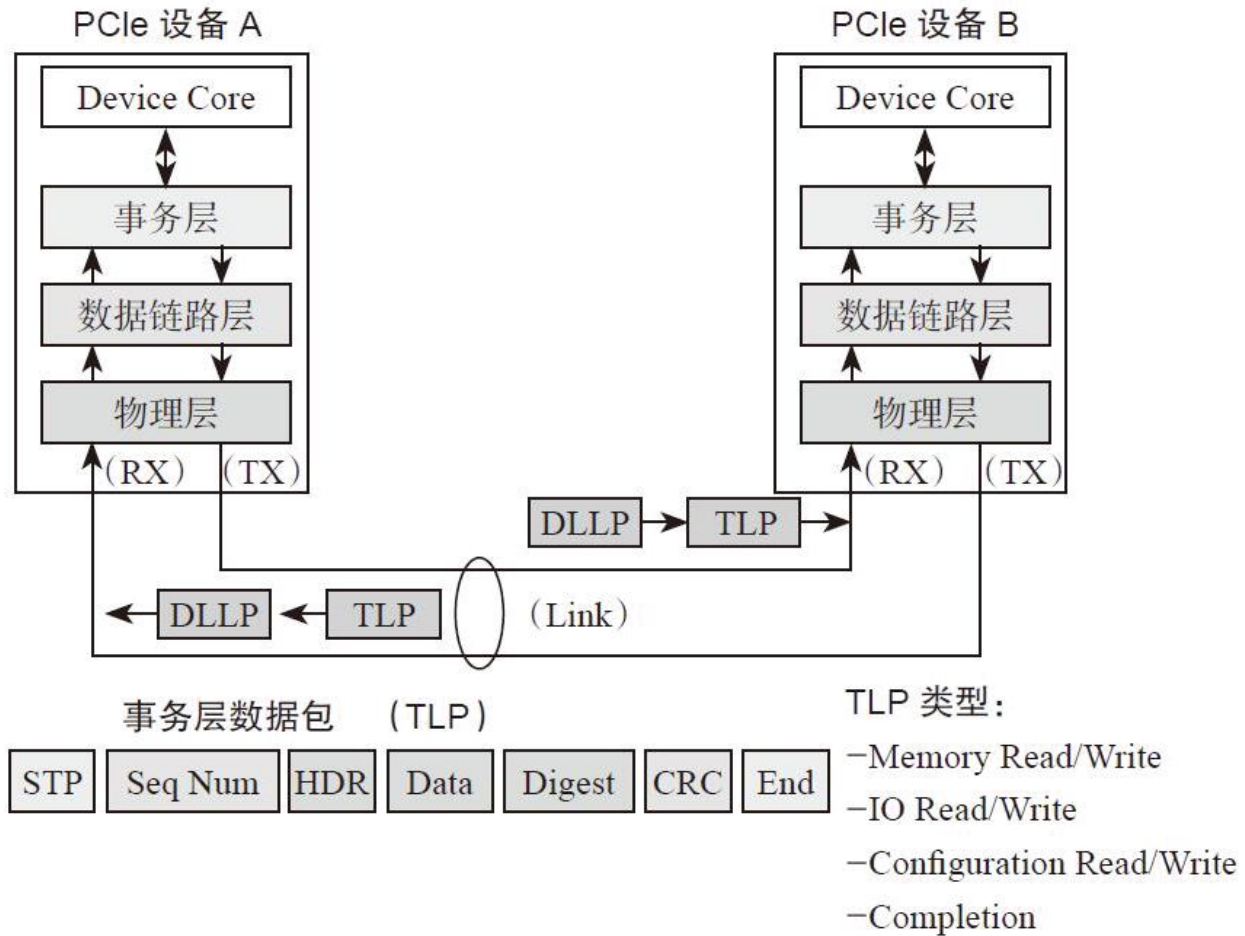


图6-30 PCIe两设备通信示意图

对PCIe，我们这里只关注事务层，因为它跟NVMe的接触是最直接、最亲密的。PCIe事务层传输的是TLP，它就是个包裹，一般由包头和数据组成，当然也有可能只有包头没有数据。NVMe传下来的数据都是放在TLP的数据部分的（Payload）。为实现不同的目的，TLP可分为以下几种类型：

- Configuration Read/Write
- I/O Read/Write
- Memory Read/Write
- Message
- Completion

注意，这个Completion跟NVMe层的Completion不是同一个东西，它们处在不同层。PCIe层的Completion TLP，是对所有Non-Posted型的TLP的响应，比如一个Read TLP，就需要Completion TLP来作为响应。

NVMe层的Completion，是对每个SQ中的命令，都需要一个Completion来作为响应。

在NVMe命令处理过程中，PCIe事务层基本只用Memory Read/Write TLP来为NVMe服务，其他类型TLP我们可以不用管。

主机发送一个Read命令，PCIe是如何服务的？接下来，结合NVMe命令处理流程，我将带着大家把图6-31看懂，看看NVMe和PCIe的事务层发生了什么。



图6-31 NVMe读命令的PCIeTrace图

这张图密密麻麻的，到底是什么？别急，蛋蛋带你一步一步把它看懂。

首先，主机准备了一个Read命令给SSD（见图6-32）。

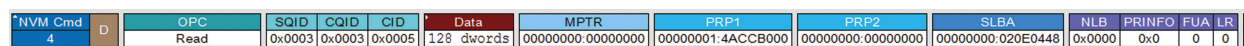


图6-32 NVMe读命令

也许你对NVMe Read命令格式不是很清楚，但从图6-32中，我们还是能得到下面的信息：主机需要从起始LBA 0x20E0448（SLBA）上读取128个DWORD（512字节）的数据，读到哪里去呢？PRP1给出内存地址是0x14ACCB000。这个命令放在编号为3的SQ里（SQID=3），CQ编号也是3（CQID=3）。我觉得知道这些就够了。相信你看了前面章节的介绍，刚才说的这些应该都能懂。

当主机把一个命令准备好放到SQ后，接下来步骤是什么呢？回想一下NVMe命令处理的八个步骤。

第一步：主机准备好命令在SQ；（完成）

第二步：主机通过写SQ的Tail DB，通知SSD来取命令。

图6-33中，上层是NVMe层，下层是PCIe的事务层，这一层我们看到的是TLP。主机想往SQ Tail DB中写入的值是5。PCIe是通过一个Memory Write TLP来实现主机写SQ的Tail DB的。

NVM	H	Device ID	QID	SQyTDBL	IO SQT QID = 3	MN	Metrics	# Link & Split Trans	Time Delta	Time Stamp		
12		006:00:0	0x0003		0x0005			1	400.000 ns	0055 . 321 622 570 s		
Link Tra	R→	5.0	TLP	Mem	MWr(32)	Length	RequesterID	Tag	Address	1st BE	Last BE	Data
235		x4	1009		010:00000	1	000:00:0	0	F7C11018	1111	0000	1 dword

图6-33 主机通过Memory Write写SQ的Tail DB

一个主机，下面可能连接着若干个Endpoint，该SSD只是其中的一个Endpoint而已，那有个问题，主机怎样才能准确更新该SSD控制器中的Tail DB寄存器呢？怎么寻址？

其实，在上电的过程中，每个Endpoint（在这里是SSD）的内部空间都会通过内存映射（Memory Map）的方式映射到主机的内存

（Memory）地址空间中，SSD控制器当中的寄存器会被映射到主机的内存地址空间，当然也包括Tail DB寄存器。主机在用Memory Write写的时候，Address只需设置该寄存器在主机内存中映射的地址，就能准确写入该寄存器。以图6-33为例，该Tail DB寄存器应该映射在主机内存地址0xF7C11018，所以主机写DB，只需指定这个映射地址，就能准确无误地写入对应的寄存器中去。

NVMe处理命令的第三步：SSD收到通知，去主机端的SQ中取指。

SSD是通过发一个Memory Read TLP到主机的SQ中取指的。可以看到，PCIe需要往主机内存中读取16个DWORD的数据。为什么是16DWORD数据？因为每个NVMe命令的大小是64个字节。从图6-34中，我们可以推断SQ 3当前的Head指向的内存地址是0x101A41100。怎么推断来的？因为SSD总是从主机的SQ Head取指的，而图6-34中，Address就是0x101A41100，所以我们有此推断。

NVM	H	Device ID	QID	CID	Address	IOSQ	OPC	PSDT	FUSE	CID	NSID	MPTR	MPTR Hi	MPTR Low	PRP1	PRP1 Low	PRP1 Hi	PRP2	PRP2 Low	PRP2 Hi
13		006 00 0	0x0003	0x0005	00000001:01A41100		Read	PRP	Normal operation	0x0005	0x00000001	0x00000000	0x00000000	0x00000000	0x4ACCB000	0x00000001				
Split Tra	R+	5.0	Mem	MRd(64)	RequesterID	CompleterID	Tag	TC	VC ID	Address	Status	Data	Metrics	# LinkTrans	Time Delta	Time Stamp				
23		x4		001.00000	006.00 0	000.00 0	2	0	0	00000001:01A41100	SC	16 dwords		2	720.000 ns	0055.321 622 970 s				
Link Tra	R+	5.0	TLP	Mem	MRd(64)	Length	RequesterID	Tag	Address	1st BE	Last BE	VC ID	Explicit ACK	Metrics	# Packets	Time Delta	Time Stamp			
236		x4	1612		001.00000	16	006.00 0	2	00000001:01A41100	1111	1111	0	Packet #372		2	720.000 ns	0055.321 622 970 s			
Link Tra	R+	5.0	TLP	Cpl	CplID	Length	RequesterID	Tag	CompleterID	Status	BCM	Byte Cnt	Lwr Addr	Data	VC ID	Explicit ACK	Metrics	# Packets	Time Delta	
237		x4	1010		010.01010	16	006.00 0	2	000.00 0	SC	0	64	0x00	16 dwords	0	Packet #374		2	21.604 us	

图6-34 SSD通过Memory Read取指

在图6-34中，SSD往主机发送了一个Memory Read的请求，主机通过Completion的方式把命令数据返回给SSD。和前面的Memory Write不同，Memory Read中不含数据，只是个请求，数据的传输需要对方发个Completion。像这种需要对方返回状态的TLP请求，我们叫它Non-Posted请求。怎么理解呢？Post有“邮政”的意思，就像你寄信一样，你往邮箱中一扔，对方能不能收到，就看快递员的素养了，反正你是把信发出去了。像Memory Write这种请求，就是Posted请求，数据传给对方，至于对方有没有处理，我们不在乎；而像Memory Read这种请求，它就必须是Non-Posted了，因为如果对方不响应（不返回数据）给我，Memory Read就是失败的。所以，每个Memory Read请求都有相应的Completion。

NVMe处理命令的第四步：SSD执行读命令，把数据从闪存中读到缓存中，然后把数据传给主机。

数据从闪存中读到缓存中，这是SSD内部的操作，跟PCIe和NVMe没有任何关系，因此，我们捕捉不到SSD的这个行为。在PCIe接口上，我们只能捕捉到SSD把数据传给主机的过程。

如图6-35所示，SSD通过Memory Write TLP把主机命令所需的128个DWORD数据写入主机命令所要求的内存中去。SSD每次写入32个DWORD，一共写了4次。正如之前所说，我们没有看到Completion TLP，合理。

NVM	D	Device ID	QID	CID	Address	CMD PRP	Data Len	Data	MN	Metrics	# Link & Split Trans	Time Delta	Time Stamp			
23		006:00:0	0x0003	0x0005	00000001:4ACCB000		0x00000080	128 dwords			4	84.000 ns	0055.321 645 294 s			
Link Tra	R+	5.0	TLP	Mem	MW(64)	Length	RequesterID	Tag	Address	1st BE	Last BE	Data	VC ID	Explicit ACK	Metrics	# Packets
299	x4	1527			011:00000	32	006:00:0	15	00000001:4ACCB000	1111	1111	32 dwords	0	Packet #469		2
Link Tra	R+	5.0	TLP	Mem	MW(64)	Length	RequesterID	Tag	Address	1st BE	Last BE	Data	VC ID	Explicit ACK	Metrics	# Packets
300	x4	1528			011:00000	32	006:00:0	16	00000001:4ACCB080	1111	1111	32 dwords	0	Packet #471		2
Link Tra	R+	5.0	TLP	Mem	MW(64)	Length	RequesterID	Tag	Address	1st BE	Last BE	Data	VC ID	Explicit ACK	Metrics	# Packets
301	x4	1529			011:00000	32	006:00:0	17	00000001:4ACCB100	1111	1111	32 dwords	0	Packet #473		2
Link Tra	R+	5.0	TLP	Mem	MW(64)	Length	RequesterID	Tag	Address	1st BE	Last BE	Data	VC ID	Explicit ACK	Metrics	# Packets
302	x4	1530			011:00000	32	006:00:0	18	00000001:4ACCB180	1111	1111	32 dwords	0	Packet #475		2

图6-35 SSD通过MemoryWrite返回数据给主机

SSD一旦把数据返回给主机，就会认为命令处理完毕，第五步就是：[SSD往主机的CQ中返回状态](#)。

如图6-36所示，SSD是通过Memory Write TLP把16个字节的命令完成状态信息写入主机的CQ中。

NVM	D	Device ID	QID	CID	Address		IOCC	Command Specific	SCQHD	SCQID	CID	P	ST	SC	SCT	M	DNR	MN
180		006:00:	0x0003	0x0005	00000001:01A51050			0x00000000	0x0023	0x0003	0x0005	1		Successful Completion	Generic Command Status	0	0	
Link Tra	R+	5.0	TLP	Mem	MW(64)	Length	RequesterID	Tag	Address		1st BE	Last BE	Data	VC ID	Explicit ACK	Metrics	# Packets	
1633	x4	2238			011:00000	4	006:00:	128	00000001:01A51050		1111	1111	4 dwords	0	Packet #2720		2	

图6-36 SSD通过MemoryWrite写CQ

SSD往主机的CQ中写入后，第六步就是：[SSD采用中断的方式告诉主机去处理CQ](#)。

SSD中断主机，NVMe/PCIe有四种方式：**Pin-Based Interrupt**、**Single Message MSI**、**Multiple Message MSI**和**MSI-X**（关于中断，具体的可以参看NVMe V1.2协议规范第171页，有详细介绍，有兴趣的可以去看看）。在图6-37中，这个例子中使用的是**MSI-X**中断方式。跟传统的中断不一样，它不是通过硬件引脚的方式，而是和正常的信息一样，通过PCIe打包把中断信息告知主机。图6-37告诉我们，SSD还是通过Memory Write TLP把中断信息告知主机，这个中断信息长度是1DWORD。

NVM		D	Device ID		QID	CID	Address		Interrupt	Type	Vector	Message	MN	Metrics	# Link & Split Trans	Time Delta	Time Stamp
181			006:00:0		0x0003	0x0005	00000000:FEE0400C			MSI-X	2	0x000049B2			1	2.272 us	0055.322 025 122 s
Link Tra		R+	5.0	TLP	Mem	MW(32)		Length	RequesterID	Tag	Address		1st BE	Last BE	Data	VC ID	Explicit ACK
1637		x4	2240			010:0000		1	006:00:0	192	FEE0400C		1111	0000	1 dword	0	Packet #2725
																Metrics	# Packets

图6-37 SSD通过Memory Write通知主机处理CQ

主机收到中断后，第七步就是：[主机处理相应的CQ](#)。这步是在主机端内部发生的事情，在Trace上我们捕捉不到这个处理过程。

最后一步，主机处理完相应的CQ后，需要[更新SSD端的CQ Head DB](#)，告知SSD CQ处理完毕。

跟前面一样，主机还是通过Memory Write TLP更新SSD端的CQ Head DB，如图6-38所示。

NVM		H	Device ID		QID		CQyHDBL		IO SQT QID = 3		MN		Metrics	# Link & Split Trans		Time Delta		Time Stamp							
184			006:00:0		0x0003				0x0006					1		-398.904 us		0055 . 322 027 394 s							
Link Tra			R→	5.0		TLP		Mem	MW(r32)		Length		RequesterID		Tag		Address		1st BE		Last BE		Data	VC ID	Explicit ACK
1658				x4		1701			010:00000		1		000:00:0		0		F7C1101C		1111		0000				
																			1 dword		0		Packet #2751		

图6-38 主机通过Memory Write更新CQ的Head DB

通过PCIe Trace，我们从PCIe的事务层看到了一个NVMe Read命令是怎么处理的，看到事务层基本都是通过Memory Write和Memory Read TLP传输NVMe命令、数据和状态等信息，看到了NVMe命令处理的八个步骤。

上面举的是NVMe读命令处理，其他命令处理过程其实差不多，这里不再赘述。

最后，我再贴出完整的Trace，相信，也希望大家不会再有一团乱麻的感觉（见图6-39）。

Cmd 4		OPC	SQID	QID	CID	Data	MPTR	PRP1	PRP2	SILBA	NLB	PRINFO	FUA	LR	DSM	ACCF	AC		
		Read	0x0003	0x0003	0x0005	128 dwords	00000000 00000000	00000001 4ACCB000	00000000 00000000	00000000 020E0448	0x0000	0x0	0	0		No frequency information provided	N		
NVM	H	Device ID	QID	CID	IO SQT QID = 3	MN	Metrics	# Link & Split Trans	Time Delta	Time Stamp									
12		006:00:0	0x0003	0x0005	0x0005			1	400.000 ns	0055 - 321 622 570 s									
Link Tra	R→	S.0	TLP	Mem	MW(r32)	Length	RequesterID	Tag	Address	1st BE	Last BE	Data	VC ID	Explicit ACK	Metrics	# Packets	Time Delta	Time Stamp	
235		x4	1009		010:00000	1	000:00:0	0	F7C11018	1111	0000	1 dword	0	Packet #371		2	400.000 ns	0055 - 321 622 570 s	
NVM	H	Device ID	QID	CID	Address	IO SQT	DPC	PRP1	FUSE	CID	Nsid	MPTR	MPTR Low	PRP1 Low	PRP1 Hi	PRP2 Low	PRP2 Hi	SL	
13		006:00:0	0x0003	0x0005	00000001 01A41100	3	Read	PRP	Normal operation	0x0005	0x00000001	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000		
Split Tra	R→	S.0	TLP	Mem	MRd(64)	Length	RequesterID	Tag	VC ID	Address	Status	Data	VC ID	Explicit ACK	Metrics	# Packets	Time Delta	Time Stamp	
23		x4	1512		001:00000	16	000:00:0	2	0	00000001 01A41100	SC	16 dwords	0	Packet #372		2	720.000 ns	0055 - 321 622 970 s	
Link Tra	R→	S.0	TLP	Mem	MRd(64)	Length	RequesterID	Tag	VC ID	Address	1st BE	Last BE	Data	VC ID	Explicit ACK	Metrics	# Packets	Time Delta	Time Stamp
236		x4	1512		001:00000	16	000:00:0	2	0	00000001 01A41100	1111	1111	16 dwords	0	Packet #372		2	720.000 ns	0055 - 321 622 970 s
Link Tra	R→	S.0	TLP	Cpl	CplD	Length	RequesterID	Tag	CompletedD	Status	BCM	Byte Cnt	Lwr Addr	VC ID	Explicit ACK	Metrics	# Packets	Time Delta	Time Stamp
237		x4	1010		010:01010	16	000:00:0	2	0	00000000	SC	0	64	0x00	0	Packet #374		2	21.604 us
NVM	D	Device ID	QID	CID	Address	Data Len	Command Specific	SQID	QID	CID	P	SC	Time Delta	Time Stamp					
23		006:00:0	0x0003	0x0005	00000001 4ACCB000	128 dwords	0x00000000	0x00000000	0x0003	0x0005	1	Successful Completion	84.000 ns	0055 - 321 645 294 s					
Link Tra	R→	S.0	TLP	Mem	MW(r64)	Length	RequesterID	Tag	Address	1st BE	Last BE	Data	VC ID	Explicit ACK	Metrics	# Packets	Time Delta	Time Stamp	
299		x4	1527		011:00000	32	006:00:0	15	00000001 4ACCB000	1111	1111	32 dwords	0	Packet #469		2	84.000 ns	0055 - 321 645 294 s	
Link Tra	R→	S.0	TLP	Mem	MW(r64)	Length	RequesterID	Tag	Address	1st BE	Last BE	Data	VC ID	Explicit ACK	Metrics	# Packets	Time Delta	Time Stamp	
300		x4	1528		011:00000	32	006:00:0	16	00000001 4ACCB000	1111	1111	32 dwords	0	Packet #471		2	84.000 ns	0055 - 321 645 378 s	
Link Tra	R→	S.0	TLP	Mem	MW(r64)	Length	RequesterID	Tag	Address	1st BE	Last BE	Data	VC ID	Explicit ACK	Metrics	# Packets	Time Delta	Time Stamp	
301		x4	1529		011:00000	32	006:00:0	17	00000001 4ACCB100	1111	1111	32 dwords	0	Packet #473		2	92.000 ns	0055 - 321 645 462 s	
Link Tra	R→	S.0	TLP	Mem	MW(r64)	Length	RequesterID	Tag	Address	1st BE	Last BE	Data	VC ID	Explicit ACK	Metrics	# Packets	Time Delta	Time Stamp	
302		x4	1530		011:00000	32	006:00:0	18	00000001 4ACCB180	1111	1111	32 dwords	0	Packet #475		2	379.444 us	0055 - 321 645 554 s	
NVM	D	Device ID	QID	CID	Address	IO SQT	Command Specific	SQID	QID	CID	P	SC	Time Delta	Time Stamp					
180		006:00:0	0x0003	0x0005	00000001 01A51050	4	0x00000000	0x0023	0x0003	0x0005	1	Successful Completion	124.000 ns	0055 - 322 024 998 s					
Link Tra	R→	S.0	TLP	Mem	MW(r64)	Length	RequesterID	Tag	Address	1st BE	Last BE	Data	VC ID	Explicit ACK	Metrics	# Packets	Time Delta	Time Stamp	
1633		x4	2238		011:00000	4	006:00:0	128	00000001 01A51050	1111	1111	4 dwords	0	Packet #2720		2	124.000 ns	0055 - 322 024 998 s	
NVM	D	Device ID	QID	CID	Address	Interrupt	Type	Vendor	Message	MN	Metrics	# Link & Split Trans	Time Delta	Time Stamp					
181		006:00:0	0x0003	0x0005	00000000 FEE0400C	MSI-X	2	0x000049B2				1	2.272 us	0055 - 322 025 122 s					
Link Tra	R→	S.0	TLP	Mem	MW(r32)	Length	RequesterID	Tag	Address	1st BE	Last BE	Data	VC ID	Explicit ACK	Metrics	# Packets	Time Delta	Time Stamp	
1637		x4	2240		010:00000	1	006:00:0	192	FEE0400C	1111	0000	1 dword	0	Packet #2725		2	2.272 us	0055 - 322 025 122 s	
NVM	H	Device ID	QID	CQyHDBL	IO SQT QID = 3	MN	Metrics	# Link & Split Trans	Time Delta	Time Stamp									
164		006:00:0	0x0003	0x0006	0x0006			1	-398.904 us	0055 - 322 027 394 s									
Link Tra	R→	S.0	TLP	Mem	MW(r32)	Length	RequesterID	Tag	Address	1st BE	Last BE	Data	VC ID	Explicit ACK	Metrics	# Packets	Time Delta	Time Stamp	
1658		x4	1701		010:00000	1	000:00:0	0	F7C1101C	1111	0000	1 dword	0	Packet #2751		2	-398.904 us	0055 - 322 027 394 s	

图6-39 NVMe读命令的PCIe Trace图

6.6 端到端数据保护

接下来，我们要说的话就是NVMe中端到端的数据保护功能，看看NVMe中的保镖是怎样为我们的数据保驾护航的。

端到端：一端是主机的内存空间，一端是SSD的闪存空间。

我们需要保护的是用户数据。主机与SSD之间，数据传输的最小单元是逻辑块（Logical Block，LB），每个逻辑块大小可以是512/1024/2048/4096等字节，主机在格式化SSD的时候，逻辑块大小就确定了，之后两者就按这个逻辑块大小进行数据交互。

数据从主机到NVM（Non-Volatile Memory，目前一般是闪存，后面我就用闪存来代表NVM），首先要经过PCIe传输到SSD的控制器，然后控制器把数据写入闪存；反过来，主机想从闪存上读取数据，首先要由SSD控制器从闪存上获得数据，然后经过PCIe把数据传送给主机，如图6-40所示。

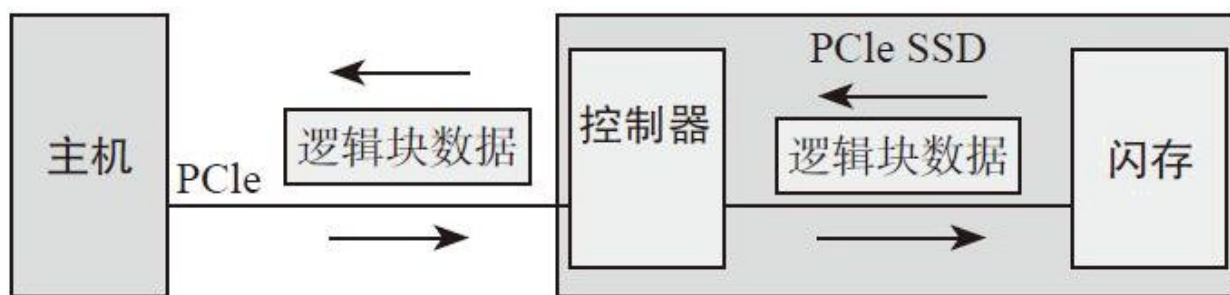


图6-40 主机与SSD之间传输数据

主机与SSD之间，数据在PCIe上传输的时候，由于信道噪声的存在（说白了就是存在干扰），可能导致数据出错；另外，在SSD内部，控制器与闪存之间，数据也可能发生错误。为确保主机与闪存之间数据的完整性，即主机写入闪存的数据与最初主机写的的数据一致，以及主机读到的数据与最初从闪存上读上来的数据一致，NVMe提供了一个端到端的数据保护功能。

除了逻辑块数据本身，NVMe还允许每个逻辑块带个助理，叫作元数据（Meta Data）。这个助理的职责，NVMe虽然没有明确要求，但如果数据需要保护，这个助理就必须能充当保镖的角色。

元数据有两种存在方式，一种是作为逻辑块数据的扩展，和逻辑块数据放一起传输，这是贴身保镖（见图6-41）。

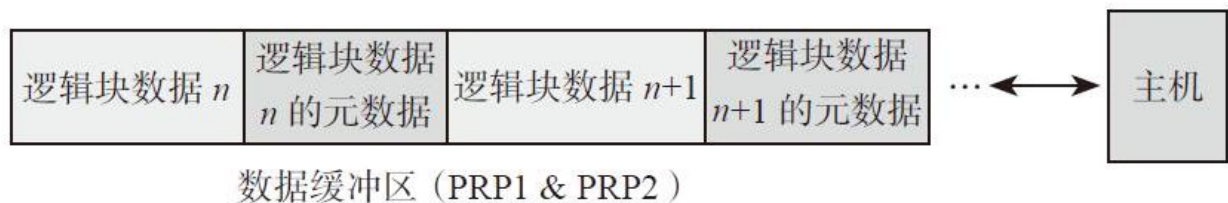


图6-41 元数据和逻辑块数据放一起传输

另外一种方式就是逻辑块数据和元数据分别传输。虽不是贴身保护，但保镖在附近时刻注意着主人的安全，属于非贴身保镖（见图6-42）。

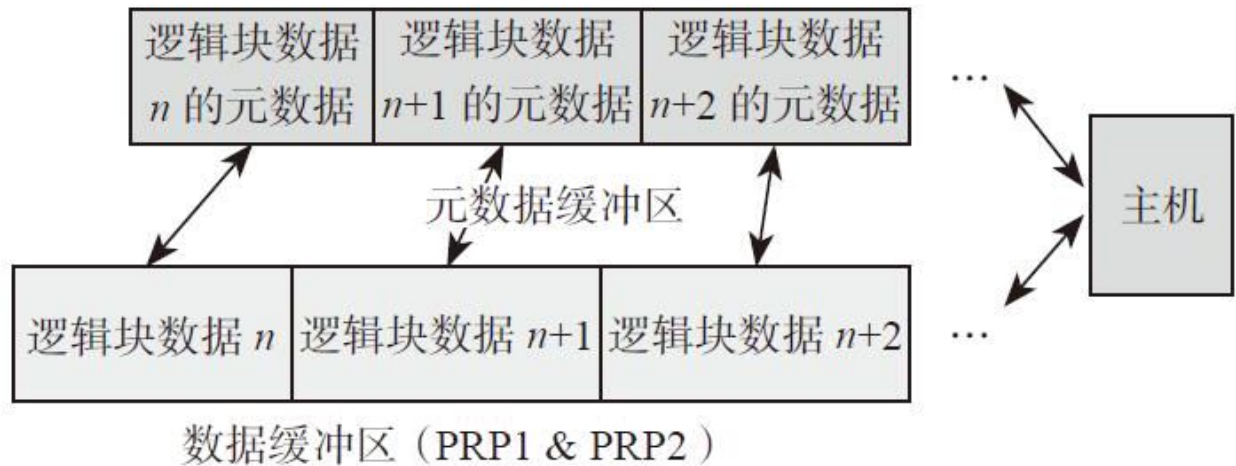


图6-42 元数据和逻辑块数据分开传输

NVMe over Fabrics只支持元数据和逻辑数据放一起，即贴身保护。

贴身保护与否，我们不关心形式，我们只关心元数据是如何保护逻辑块数据的。NVMe要求每个逻辑块数据的保镖配备下面这把武器（见图6-43）。

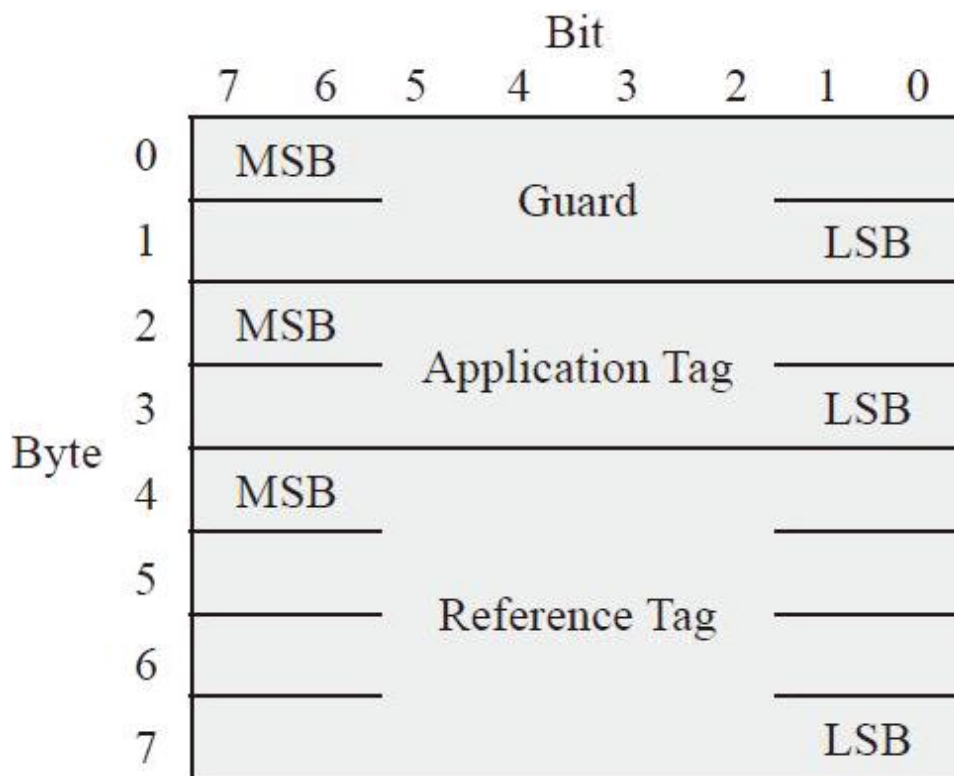


图6-43 数据保护信息格式

其中：

·Guard: 16比特的CRC（Cyclic Redundancy Check），它是逻辑块数据算出来的；

·Application Tag: 这块区域对控制器不可见，为主机所用；

·Reference Tag: 将用户数据和地址（LBA）相关联，防止数据错乱。

CRC校验能够检测出数据是否有错，后者则是保证数据不会出现张冠李戴的问题，比如我读LBA x，结果却读到了LBA y的数据。NVMe数据保护机制能发现这类问题。

配了保镖的数据如图6-44所示（以512字节的数据块为例）。

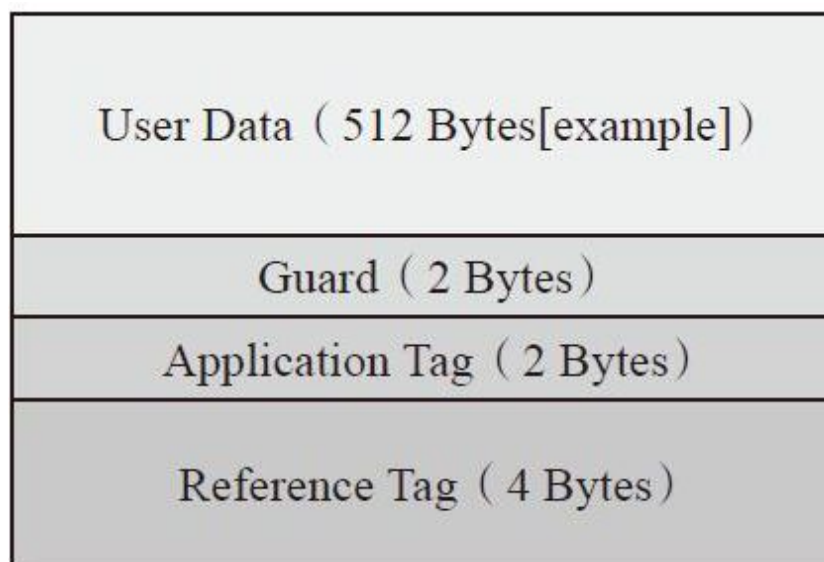


图6-44 带有保护信息的逻辑数据块

在主机与SSD数据传输过程中，NVMe可以让每个逻辑块数据都带上保镖，可以让它们不带保镖，也可以在某个治安差的地方把保镖带上，然后在治安环境好的地方不用保镖。

主机向SSD写入数据，不带保镖（见图6-45）。

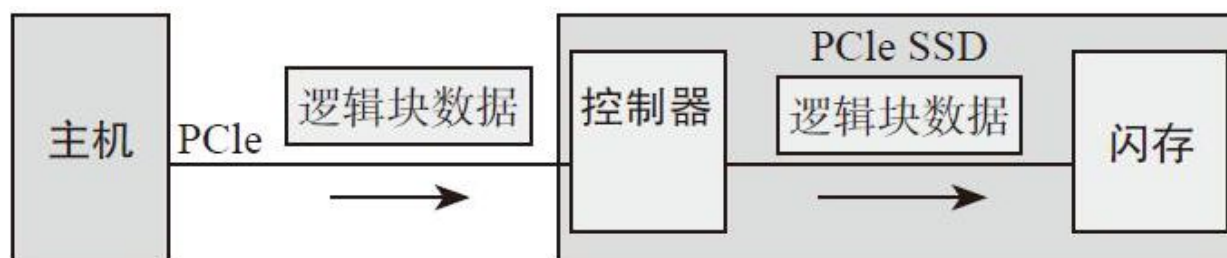


图6-45 不带数据保护信息

什么情况下可以不带保镖？

如果你是普通人，完全没有必要配保镖，原因有：①你请不起保镖；②谁有空来伤害你呢？③太平盛世。

如果是无关紧要的数据（如小电影），完全没有必要进行端到端的保护，毕竟数据保护需要传输额外的数据（每个逻辑数据块需要至少额外8字节的数据保护信息，有效带宽减少），还需要SSD做额外的数据完整性校验（耗时，性能变差）。最关键的是在PCIe通道上，本

来就有LCRC的保护，有必要的话还可以使能ECRC，这个跟NVMe关系不大，就不展开了。

主机向SSD写入数据，全程带上保镖的情况（见图6-46）。



图6-46 带数据保护信息数据写流程

图6-46中的PI（Protection Information，保护信息）就是传说中的保镖。

主机数据通过PCIe传输到SSD控制器时，SSD控制器会重新计算逻辑块数据的CRC，与保镖的CRC比较，如果两者匹配，说明数据传输是没有问题的；否则，数据就是有问题的，这个时候，SSD控制器就会给主机报错。

除了CRC校验，还要检测有没有张冠李戴的问题，通过检测Reference Tag，看看这个没有CRC问题的数据是不是该主机写命令对应的数据，如果不匹配，同样需要向主机报错。

如果数据检测没有问题，SSD控制器会把逻辑块数据和PI一同写入闪存中。将PI一同写入闪存中有什么意义呢？在读的时候有意义，如图6-47所示。

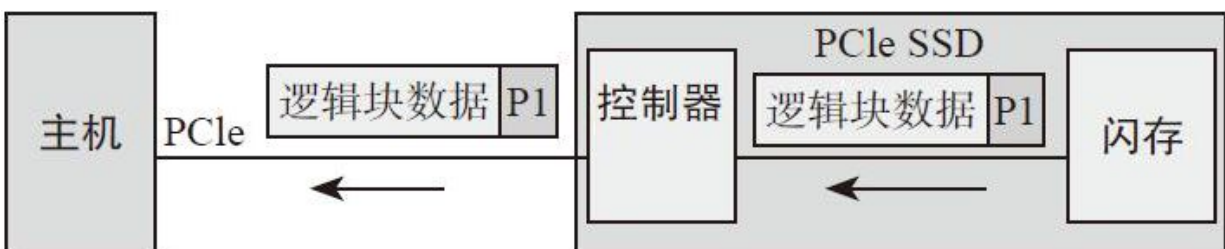


图6-47 带数据保护信息数据读流程

SSD控制器读闪存的时候，会对读上来的数据进行CRC校验，如果写入的时候带有PI，这个时候就能检测出读上来的数据是否正确，从

而决定这个数据要不要传给主机。有人要说，对闪存来说，数据不是受ECC保护吗？为什么还要额外进行数据校验？没错，写入闪存中的数据是受ECC保护，这个没有问题，但在SSD内部，数据从控制器到闪存之间，一般都要经过DRAM或者SRAM，在之前SSD控制器写入闪存，或者这个时候从闪存读数据到SSD控制器，可能就会发生比特翻转之类的小概率事件，从而导致数据不正确。如果在NVMe层再做个CRC保护，这类数据错误就能被发现了。

除了数据在SSD内发生反转，由于固件问题或者别的原因，还是会出现数据张冠李戴的问题：数据虽然没有CRC错误，但是它不是我们想要的数据。因此，还需要做Reference Tag检测。

SSD控制器通过PCIe把数据传给主机，主机端也会对数据进行校验，看SSD返回的数据是否有错。

主机往SSD写入数据，半程带保镖的情况（见图6-48）。

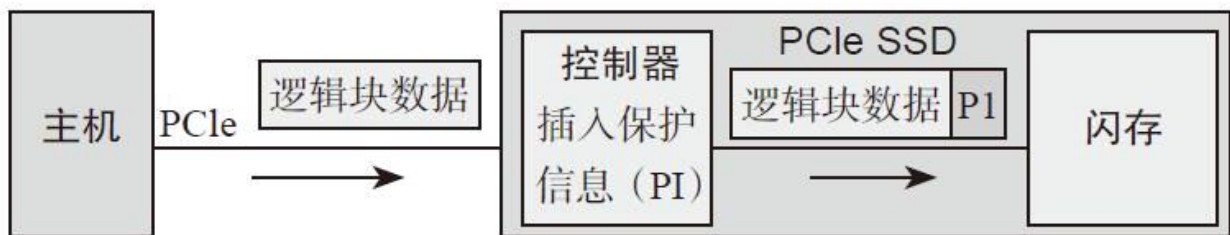


图6-48 SSD内部加入数据保护信息

这种情况，主机与控制器端之间是没有数据保护的，因为PCIe已经能提供数据完整性保证了。但在SSD内部，控制器到闪存之间，由于乱七八糟的原因（数据反转，LBA数据不匹配），存在数据错误的可能，NVMe要求SSD控制器在把数据写入闪存前，计算好数据的PI，然后把数据和PI一同写入闪存。

SSD控制器读闪存的时候，会对读上来的数据进行PI校验，如果没有问题，剥除PI，然后把逻辑块数据返回给主机；如果校验失败，说明数据存在问题，SSD需要向主机报错，如图6-49所示。

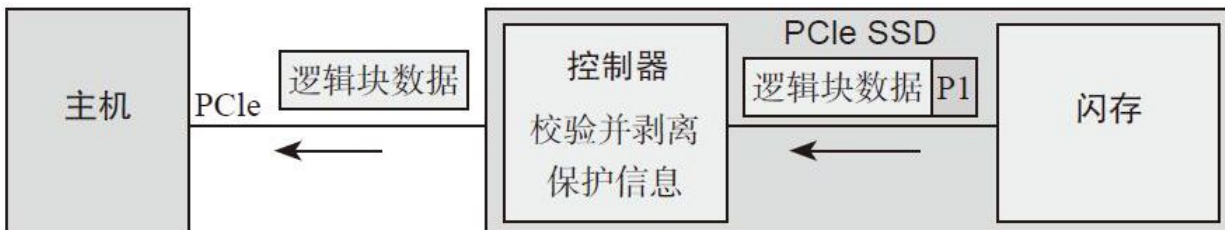


图6-49 SSD内部根据数据保护信息验证数据

数据端到端保护是NVMe的一个特色，其本质就是在数据块中加入CRC和数据块对应的LBA等冗余信息，SSD控制器或者主机端利用这些信息进行数据校验，然后根据校验结果执行相应的操作。加入这些检错信息的好处是能让主机与SSD控制器及时发现数据错误，副作用就是：

- 1) 每个数据块需要额外的至少8字节的数据保护信息，有效带宽减少：数据块越小，带宽影响越大。
- 2) SSD控制器需要做数据校验，影响性能。

但是，我觉得这二个副作用的影响是微乎其微的，跟数据安全性相比，这又算得了什么呢？

6.7 Namespace

什么是Namespace（以下简称NS）？

一个NVMe SSD主要由SSD控制器、闪存空间和PCIe接口组成。如果把闪存空间划分成若干个独立的逻辑空间，每个空间逻辑块地址（LBA）范围是0到N-1（N是逻辑空间大小），这样划分出来的每一个逻辑空间我们就叫作NS。对SATA SSD来说，一个闪存空间只对应着一个逻辑空间，与之不同的是，NVMe SSD可以是一个闪存空间对应多个逻辑空间。

每个NS都有一个名称与ID，如同每个人都有名字和身份证号码，ID是独一无二的，系统就是通过NS的ID来区分不同的NS。

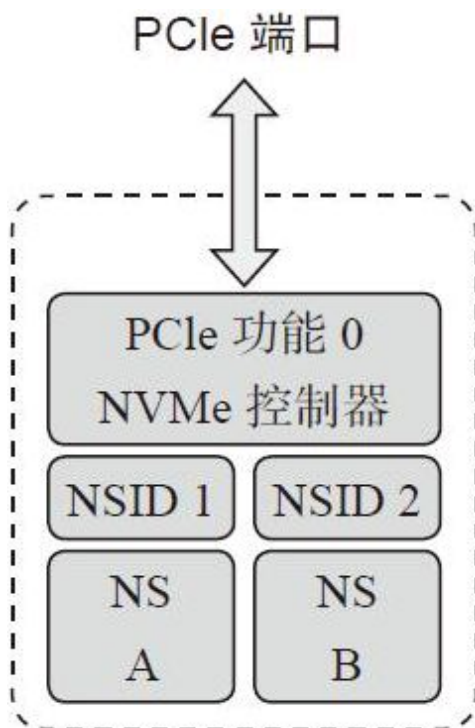


图6-50 两个NS

如图6-50所示，整个闪存空间划分成两个NS，名字分别是NS A和NS B，对应的NS ID分别是1和2。如果NS A大小是M（以逻辑块大小为单位），NS B大小是N，则它们的逻辑地址空间分别是0到M-1和0到N-1。主机读写SSD，都是要在命令中指定读写的是哪个NS中的逻辑

块。原因很简单，如果不指定NS，对同一个LBA来说，假设就是LBA 0，SSD根本就不知道去读或者写哪里，因为有两个逻辑空间，每个逻辑空间都有LBA 0。

如同我只说德州，如果不告诉你是哪个国家的，你怎知道我说的是美国德州还是山东德州。

一个NVMe命令一共64字节，其中Byte[7: 4]指定了要访问的NS，如表6-5所示。

表6-5 NVMe命令中NS域

字节	描述
63:60	命令 Dword15 (CDW15): 命令相关
59:56	命令 Dword14 (CDW14): 命令相关
55:52	命令 Dword13 (CDW13): 命令相关
51:48	命令 Dword12 (CDW12): 命令相关
47:44	命令 Dword11 (CDW11): 命令相关
43:40	命令 Dword10 (CDW10): 命令相关
39:32	PRP Entry 2 (PRP2): 命令中第二个地址条目 (如果有用到的话)
31:24	PRP Entry 1 (PRP1): 命令中第一个地址条目
23:16	MetadataPointer (MPTR): 连续元数据缓冲区地址
(续)	
字节	描述
15:8	保留
7:4	NamespaceIdentifier (NSID)
3:0	命令 Dword0 (CDW0): 所有命令都用

对每个NS来说，都有一个4KB大小的数据结构来描述它。该数据结构描述了该NS的大小，整个空间已经写了多少，每个LBA的大小，端到端数据保护相关设置，以及该NS是属于某个控制器还是几个控制器可以共享等。

NS由主机创建和管理，每个创建好的NS，从主机操作系统角度来看，就是一个独立的磁盘，用户可在每个NS做分区等操作。

下例中，整个闪存空间划分成两个NS，NS A和NS B，操作系统看到两个完全独立的磁盘，如图6-51所示。

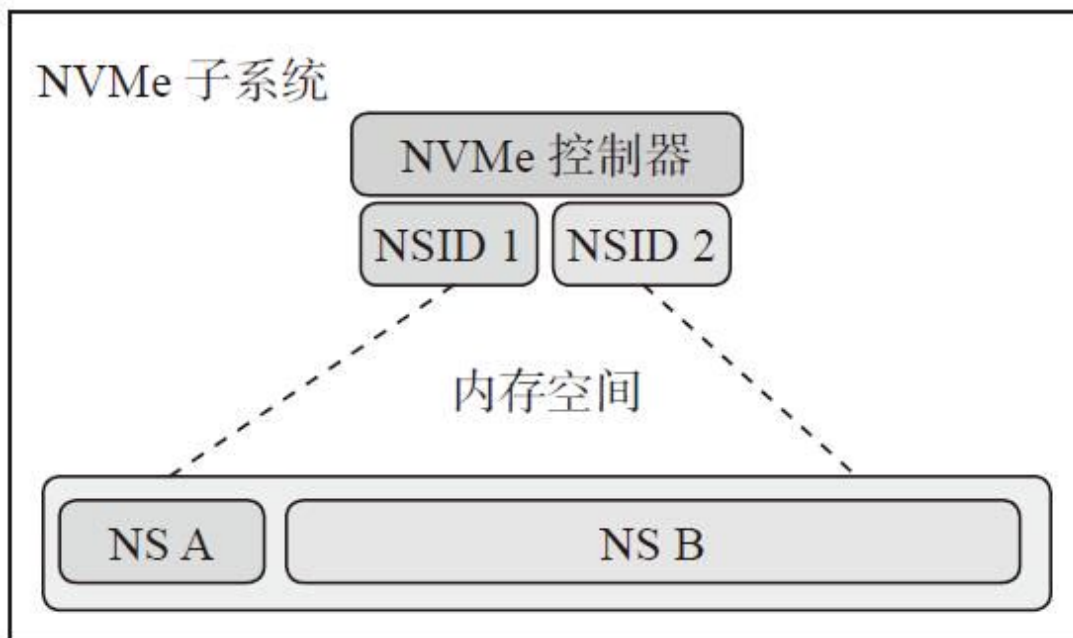


图6-51 NVMe子系统中有两个NS

每个NS是独立的，逻辑块大小可以不同，端到端数据保护配置也可以不同：你可以让一个NS使用保镖，另一个NS不使用保镖，再一个NS半程使用保镖（见6.6节）。

其实，NS更多是应用在企业级，可以根据客户不同需求创建不同特征的NS，也就是在一个SSD上创建出若干个不同功能特征的磁盘（NS）供不同客户使用。

NS的另外一个重要使用场合是：SR-IOV。

什么是SR-IOV？英文全称为Single Root-IO Virtualization，SR-IOV技术允许在虚拟机之间高效共享PCIe设备，并且它是在硬件中实现的，可以获得能够与本机性能媲美的IO性能。单个IO资源（单个SSD）可由许多虚拟机共享。共享的设备将提供专用的资源，并且还使用共享的通用资源。这样，每个虚拟机都可访问唯一的资源。

如图6-52所示，该SSD作为PCIe的一个Endpoint，实现了一个物理功能（Physical Function，PF），有4个虚拟功能（Virtual Function，VF）关联该PF。每个VF，都有自己独享的NS，还有公共的NS（NSE）。此功能使得虚拟功能可以共享物理设备，并在没有CPU和虚拟机

管理程序软件开销的情况下执行IO。关于SR-IOV的更多知识，这里就不展开了，我们只需知道NVMe中的NS有用武之地就可以。

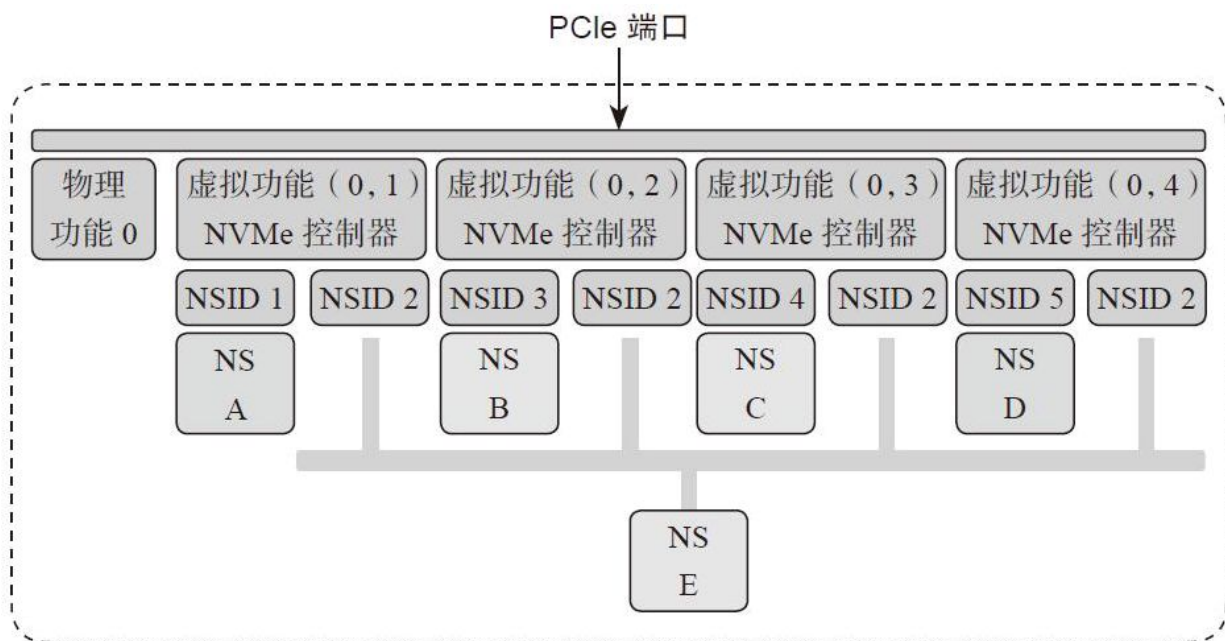


图6-52 SR-IOV

对一个NVMe子系统来说，除了包含若干个NS，还可以有若干个SSD控制器。注意，这里不是说一个SSD控制器有多个CPU，而是说一个SSD有几个实现了NVMe功能的控制器。

如图6-53所示，一个NVMe子系统包含了两个控制器，分别实现不同功能（也可以是相同功能）。整个闪存空间分成3个NS，其中NS A由控制器0（左边）独享，NS C由控制器1（右边）独享，而NS B是两者共享。独享的意思是说只有与之关联的控制器才能访问该NS，别的控制器是不能对其进行访问的，图6-53中控制器0是不能对NS C进行读写操作的，同样，控制器1也不能访问NS A；共享的意思是说，该NS（这里是NS B）是可以被两个控制器共同访问的。对共享NS，由于几个控制器都可以对它进行访问，所以要求每个控制器对该NS的访问都是原子操作，从而避免同步问题。

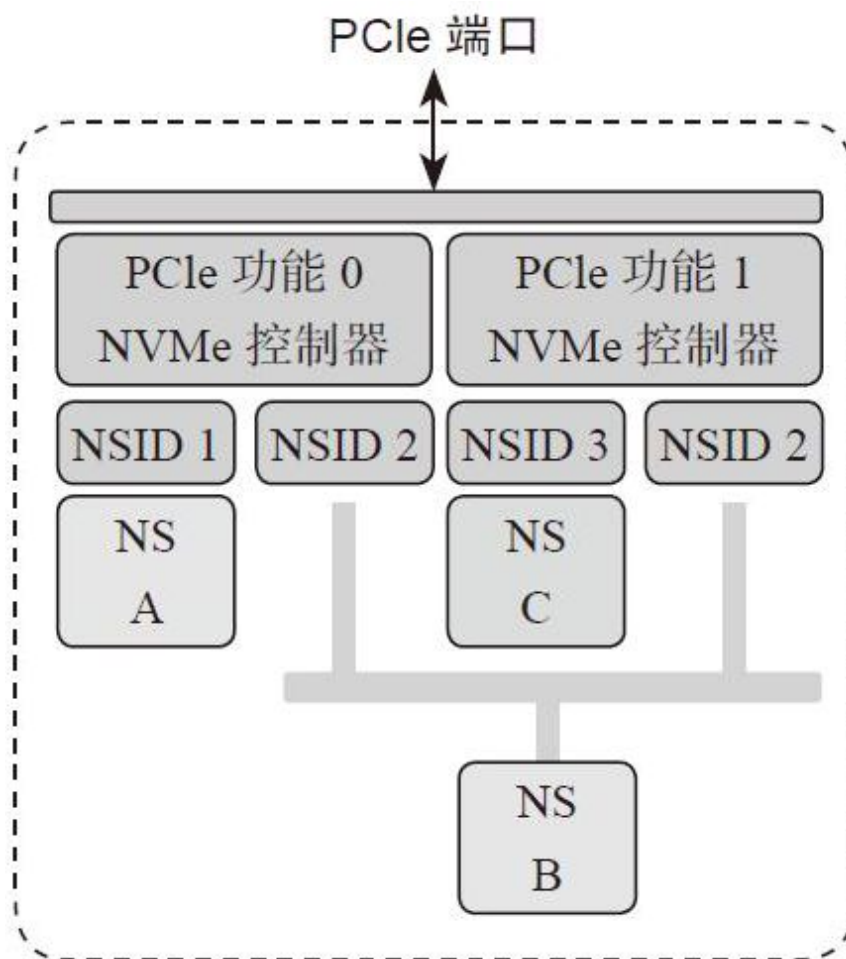


图6-53 NVMe子系统中有两个控制器

事实上，一个NVMe子系统，除了可以有若干个NS，除了可以有若干个控制器，还可以有若干个PCIe接口。

与前面的架构不一样，图6-54的架构是每一个控制器都有自己的PCIe接口，而不是两者共享一个。Dual Port，双端口，在SATA SSD上没有见过吧。这两个接口往上有可能连着同一个主机，也可能连着不同的主机。现在能提供Dual PCIe Port的SSD接口只有SFF-8639（关于这个接口，可参看www.ssdfans.com 站内文章《SFF-8639接口来袭》），也叫U.2，它支持标准的NVMe协议和Dual-Port。

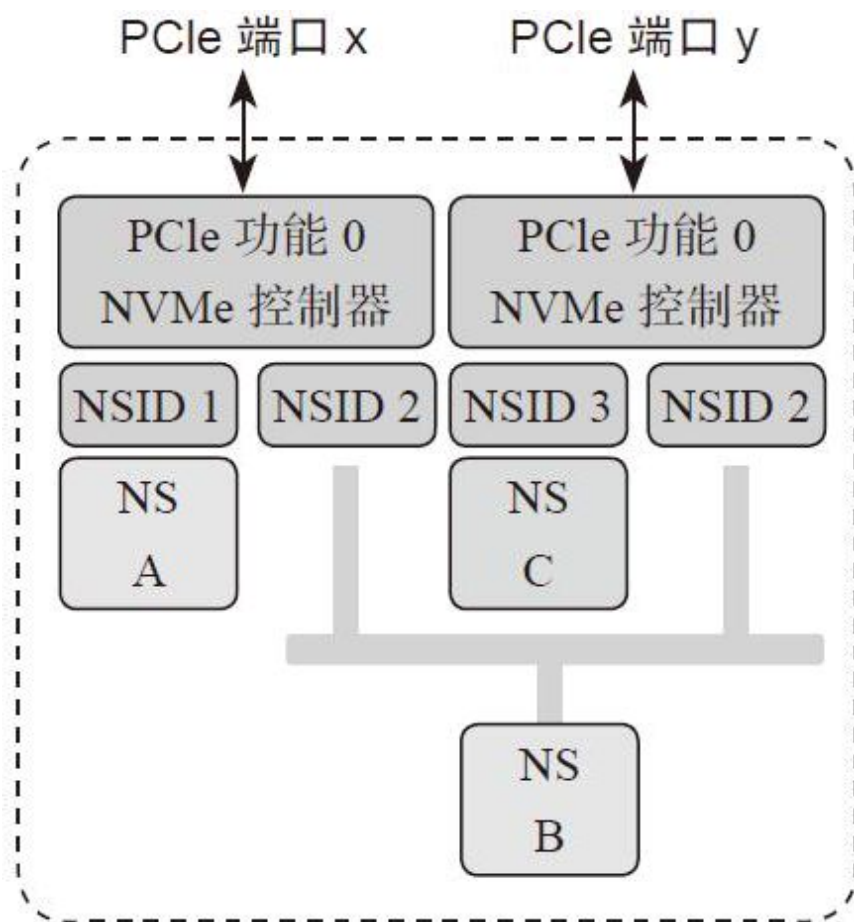


图6-54 双控制器和双端口NVMe子系统

图6-55是两个PCIe接口连着一个主机的情况。

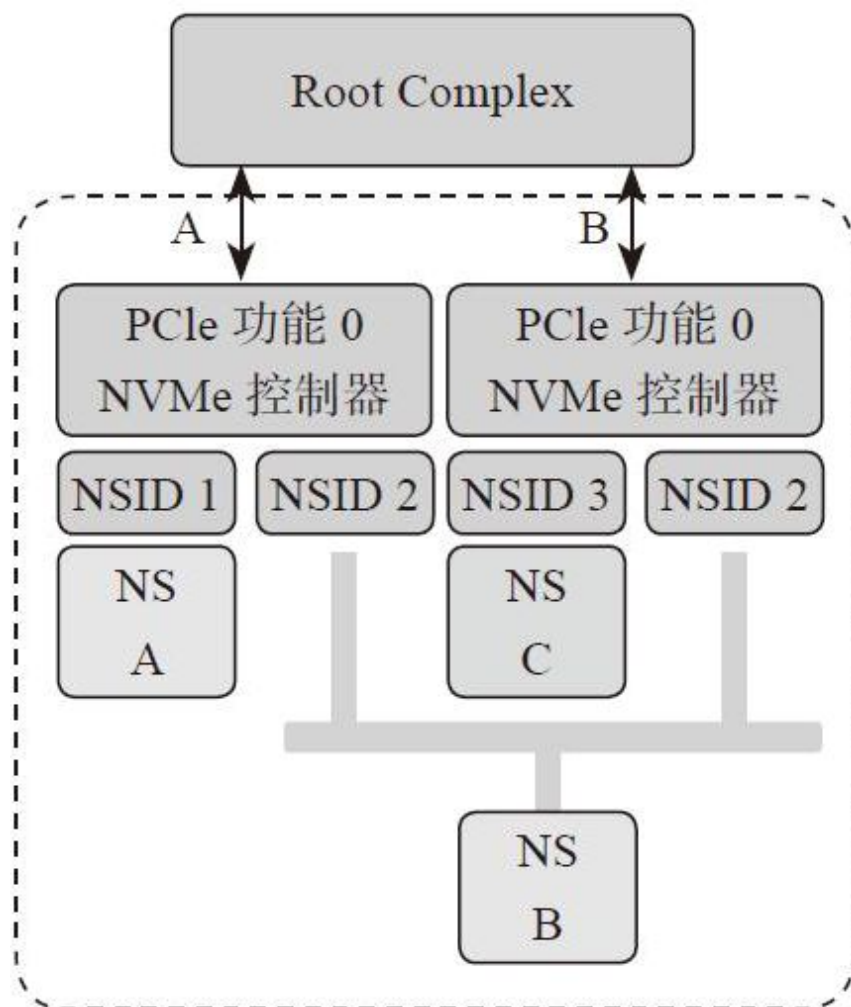


图6-55 双端口子系统连接主机

为什么要这么玩？

我认为，一方面，主机访问SSD，可以双管齐下，性能可能更好点。不过对访问NS B来说，同一时刻只能被一个控制器访问，双管齐下又如何。考虑到还可以同时操作NS A和NS C，性能或多或少会有所提升。

我觉得，更重要的是，这种双接口冗余设计可以提升系统可靠性。假设PCIe A接口出现问题，这个时候主机可以通过PCIe B无缝衔接，继续对NS B进行访问。当然了，NS A是无法访问了。

如果主机突然死机怎么办？在一些很苛刻的场景下是不允许主机宕机的。但是，是电脑总有死机的时候，怎么办？最直接有效的办法

还是采用冗余容错策略：SSD有两个控制器，有两个PCIe接口，那么我主机也弄个双主机，一个主机挂了，由另一个主机接管任务，继续执行，如图6-56所示。

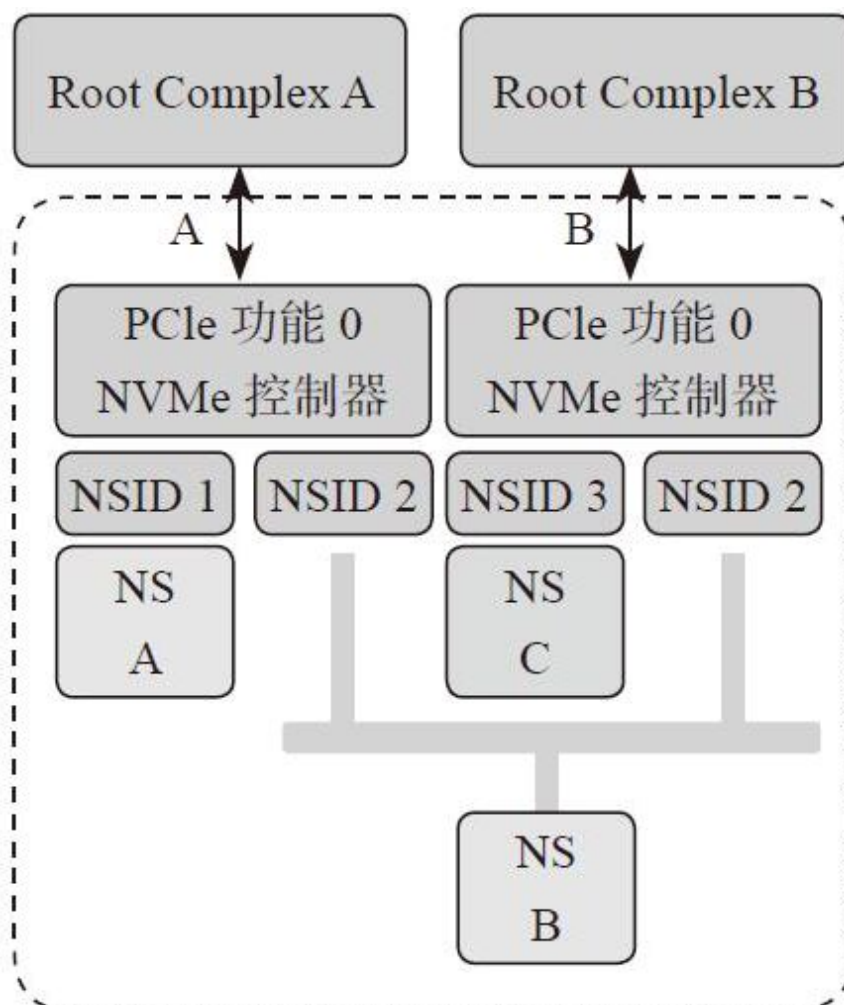


图6-56 双端口双主机系统

我们来看一个双端口的真实产品。

2015年，OCZ发布了业界第一个具有双端口的PCIe NVMe的SSD：Z-Drive 6000系列（见图6-57）。



图6-57 双端口SSD: Z-Drive 6000

物理上，这些SSD都有两个PCIe端口，但可以通过不同的固件，实现单端口和双端口功能。

每个端口可以连接独立的主机，主机端有两个独立的数据通道（Data Path）对闪存空间进行访问，如果其中一个数据通道发生故障，OCZ的主机热交换（Hot-swap）技术能让另外一个主机无缝低延时地接管任务。有些应用，比如银行金融系统、在线交易处理

（OnLine Transaction Processing, OLTP）、在线分析处理（OnLine Analytical Processing, OLAP）、高性能计算（High Performance Computing, HPC）、大数据等，对系统可靠性和实时性要求非常高，这个时候，带有双端口的SSD就能派上用场了，如图6-58所示。

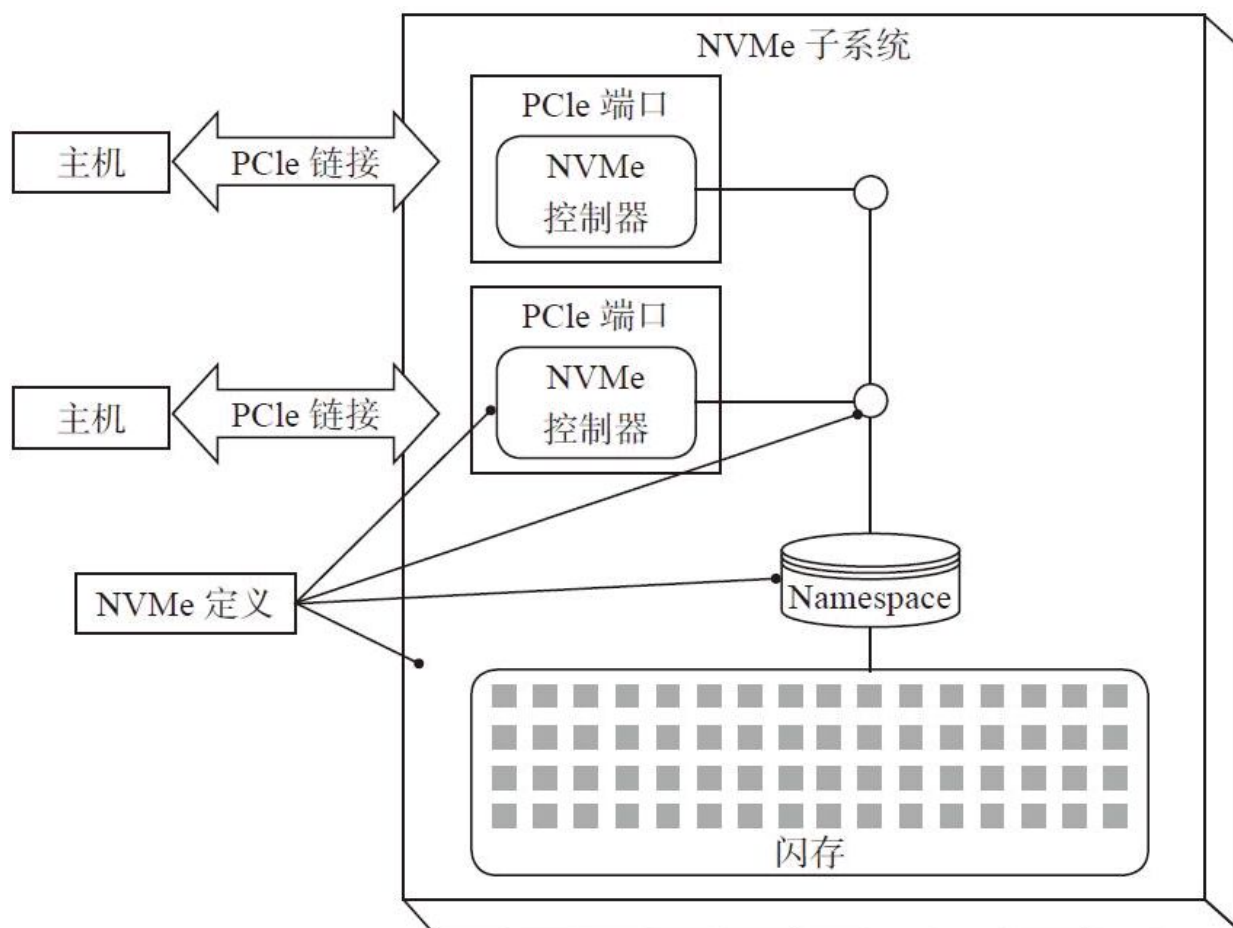


图6-58 双端口连接双主机系统

带有双端口的这种SSD，主要是面向企业用户，特别是上面提到的那些应用行业。对我们普通用户来说，我感觉就没有这个必要使用双端口了。

多NS，多控制器，多PCIe接口，给NVMe SSD开发者以及存储架构师带来很大的发挥空间。给不同的NS配置不同的数据保护机制，或者虚拟化，或者使用冗余容错提高系统可靠性，抑或别的设计，NVMe提供了这些基础设施，怎么玩就看你的想象力了。

6.8 NVMe over Fabrics

注：本书NVMe over Fabrics部分的内容来自MemBlaze的路向峰先生，SSDFans获得其授权收录其文章，感谢路向峰先生对我们的信任。

NVMe是针对新型的Non-Volatile Memory（比如闪存、3D XPoint等）而量身定制的，对于今天的应用来说，基于NVMe协议的SSD可以提供对性能、延迟、IO协议栈开销的完美优化。一个SSD高达几十万甚至上百万IOPS的随机读写性能可以使单机应用用户体验飞速提升，但往往单机应用没法充分地填满这么多带宽。

NVMe SSD目前的主要应用之一是全闪存阵列，但是PCIe接口并不适合存储设备的横向扩展（Scale Out）：想象一下如何把几百块NVMe SSD通过PCIe接入一个存储池中。

按照传统的模式，将少量的NVMe SSD组成存储节点，再通过iSCSI连接到前端，如图6-59所示。

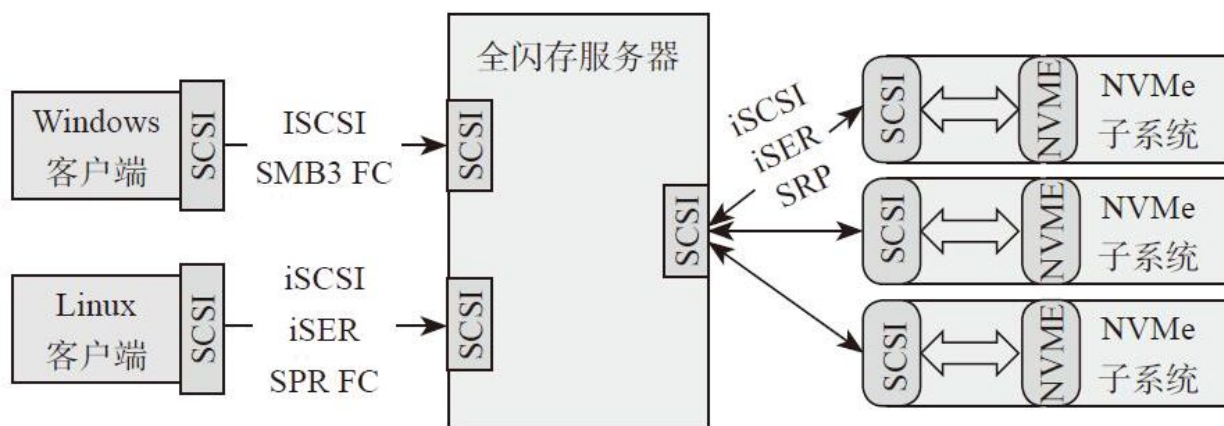


图6-59 传统存储连接方式

这样的方式带来一个问题，NVMe未来的小目标是时延（Latency）做到10 μ s以内，而iSCSI协议（或者iSER、SRP）的时延是100 μ s，如图6-60所示。

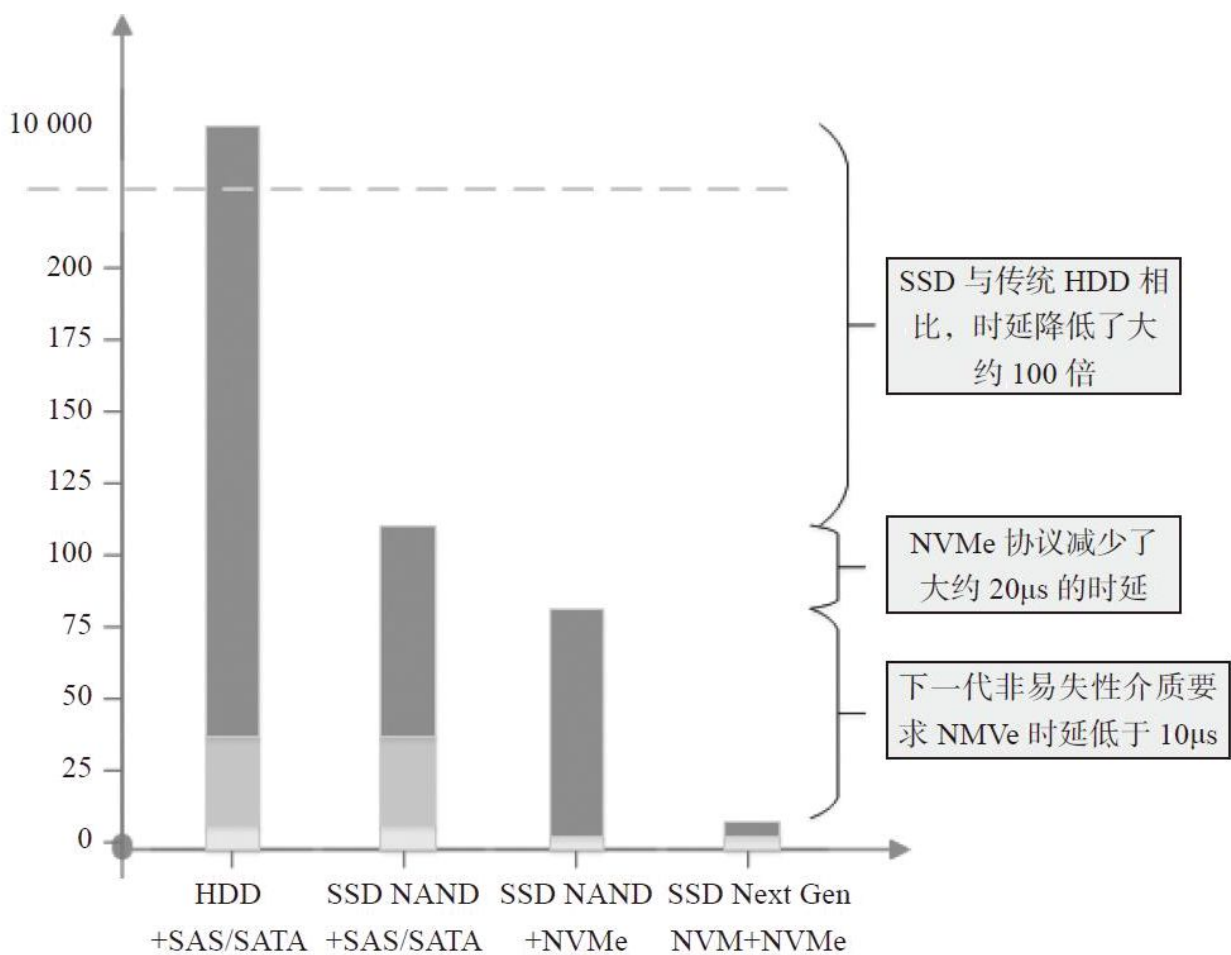


图6-60 存储设备时延的进化

把一辆法拉利放到北京早高峰的西直门立交桥上，你什么意思？

NVMe over Fabrics就是为了解决这个问题而生（见图6-61）。

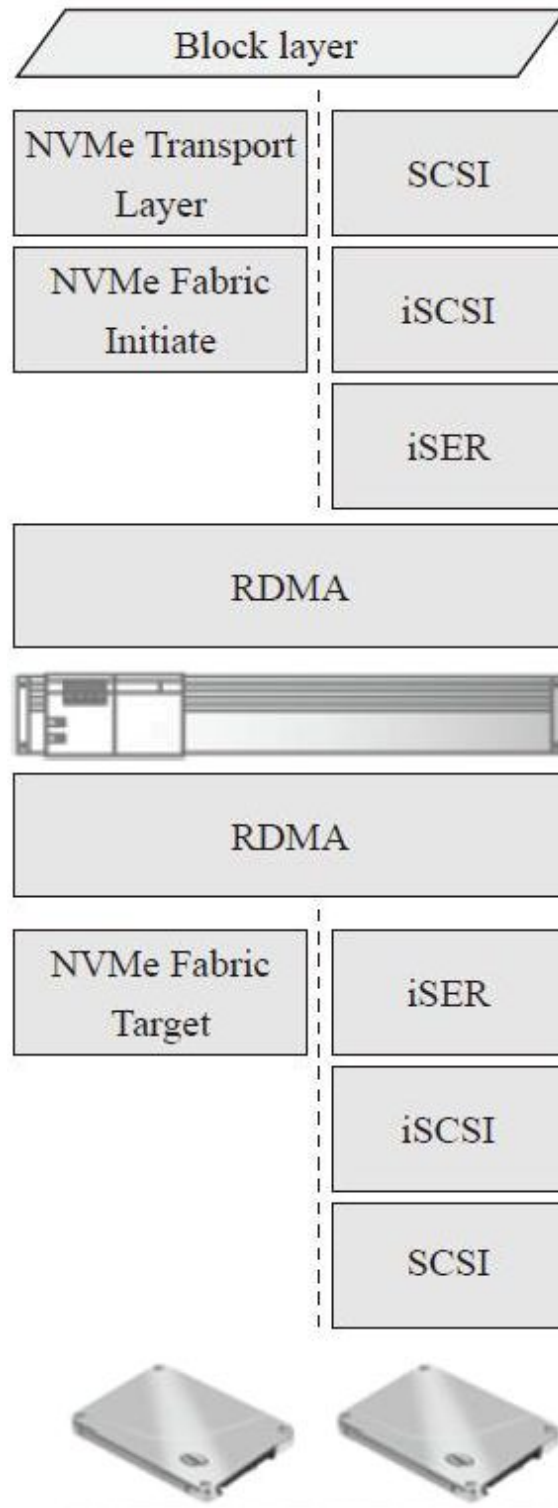


图6-61 NVMe over Fabrics（左）与传统方式协议栈（右）比较

NVMe over Fabrics协议定义了使用各种通用的事务层协议来实现NVMe功能的方式。在协议中所指的事务层包括了RDMA、

FibreChannel、PCIe Fabrics等实现方式。

由于NVMe over Fabrics协议的这种灵活性，它可以非常方便地生长在各个主流的事务层协议中。不过由于不同的互联协议本身的特点不同，因此基于各种协议的NVMe over Fabrics的具体实现都是不同的。一些协议本身的协议开销较大，另一些需要专用的硬件网络设备，客观上限制了NVMe over Fabrics协议在其中的推广。

虽然有众多可以选择的互联方式，但这些互联方式按照接口类型可分成三类：内存（Memory）型接口、消息（Message）型接口和消息内存混合（Memory&Message）型接口。相应的互联类型和例子如图6-62所示。

在这些众多的事务层协议中，重点介绍一下RDMA。RDMA（Remote Direct Memory Access，远程DMA）通过网络把数据直接传入计算机的存储区，降低了CPU的处理工作量。当一个应用执行RDMA读或写请求时，不执行任何数据复制。在不需要任何内核内存参与的情况下，RDMA请求会直接从运行在用户空间的应用中发送到本地网卡，然后经过网络传送到远程网卡，如图6-63所示。

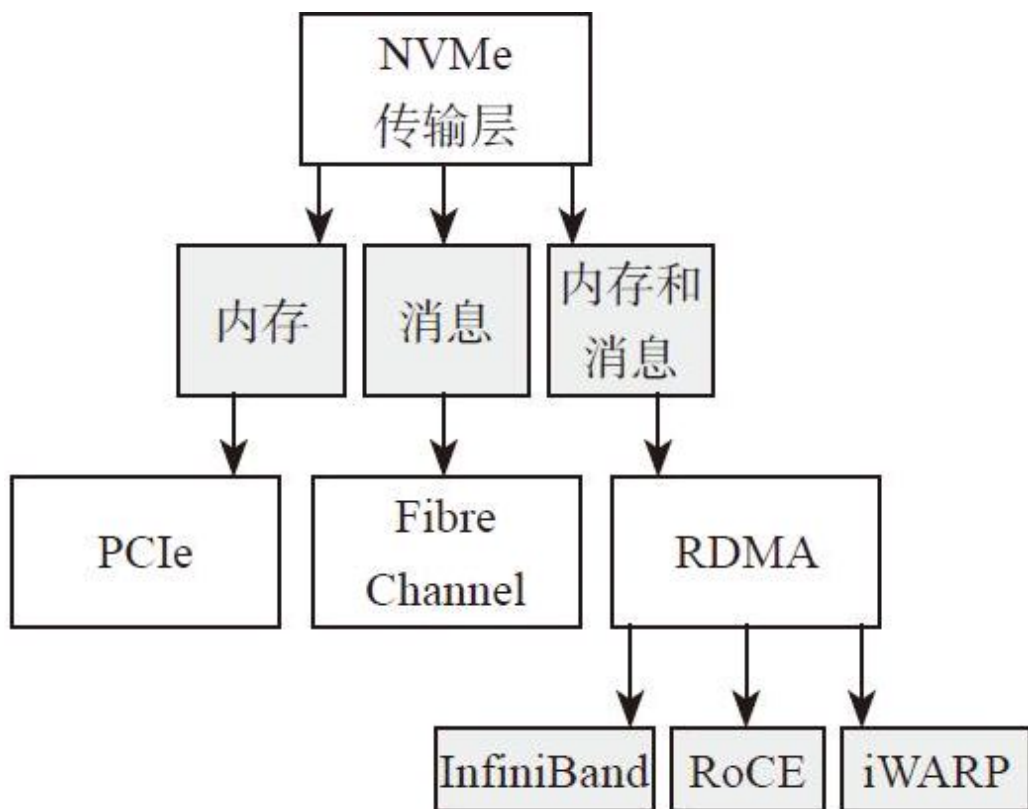


图6-62 存储互联方式的分类

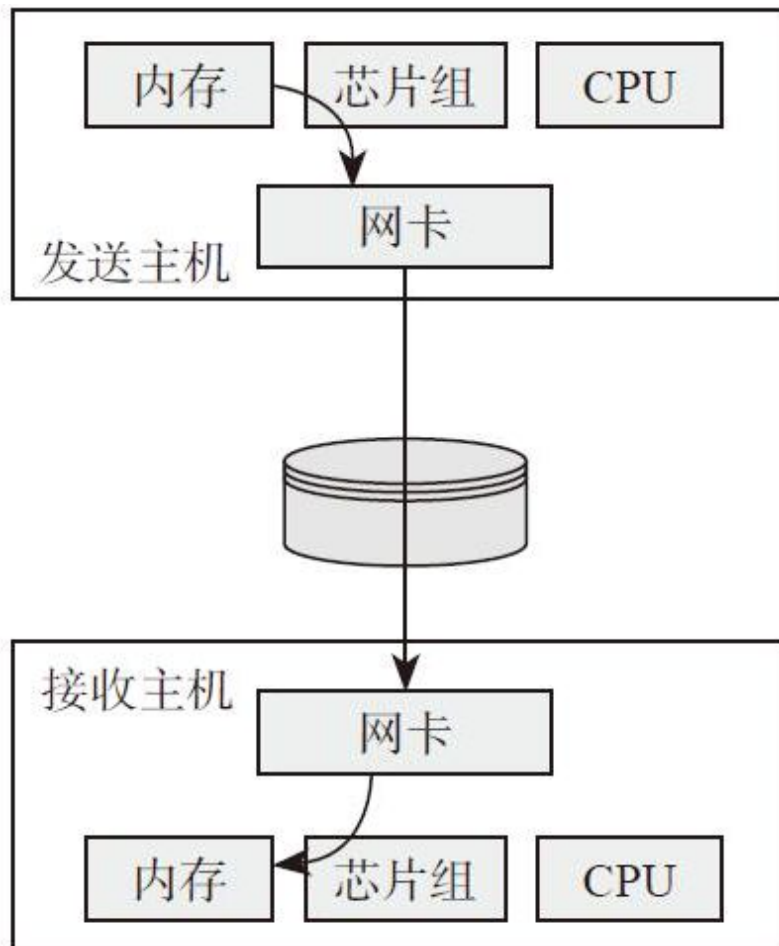


图6-63 用RDMA实现数据传输

RDMA对于NVMe over Fabrics协议的便利性体现在以下几个方面：

- 提供了低延迟、低抖动和低CPU使用率的事务层协议；
- 最大限度利用硬件加速，避免软件协议栈的开销；
- 定义了丰富的可异步访问的接口机制，这对于提高IO性能是至关重要的。

RDMA设计初衷就是为了高性能、低延迟访问远端节点的，并且它的语义非常类似本地DMA的过程，因此很自然就可以将RDMA作为NVMe协议的载体，实现基于网络的NVMe协议。

但是，毕竟基于网络的传输模型与本地的PCIe传输模型还有种种差异，因此将NVMe协议扩展到互联层面需要解决一系列问题。所以，综合RDMA、FC等各种不同事务层协议的特点，NVMexpress Inc.提出了NVMe over Fabrics协议，这是一个完整的网络高效存储协议。

对于NVMe over Fabrics协议来说，要解决下面几个问题：

- 1) 提供对于不同互联透明的消息和数据的封装格式；
- 2) 将NVMe进行操作所需要的接口方式映射到互连网络；
- 3) 解决互连网络的节点发现、多路径等互联引入的新问题。

NVMe over Fabrics协议定义了一整套数据封装方案，与传统的NVMe协议相比，这套封装方案针对互联做了一些调整和适配。NVMe定义了一套异步的由软件驱动硬件执行相应动作的异步操作机制，发送和完成包仅仅携带必要的描述，而真正的数据和SGL描述符都是放在内存中并且由硬件通过DMA方式取得的。这是基于PCIe的DMA操作延迟很短（1us）的前提设计的。然而在互联协议中，节点之间的交互时间大大增加，为了减少两个节点之间不必要的交互，发送请求可以直接携带附加的数据或SGL描述符，完成请求也可以携带需要回传的数据，节约了两者之间交互的负担。

图6-64为NVMe Fabric命令数据包。

NVMe Fabric 命令数据包	
Command ID	可选的附加 SGL 或者命令数据
OpCode	
NSID	
Buffer Address (PRP/SGL)	
Command Parameters	

图6-64 NVMe Fabric命令数据包

NVMe Fabric 响应数据包	
Command Parameters	可选的命令数据
SQ Head Ptr	
Command Status	
Command ID	

图6-65 NVMe Fabric响应数据包

与此同时，为了减少系统交互，在NVMe over Fabrics协议中，完成队列没有使用流控机制，因此需要主机在发送新命令之前确保完成队列有足够的可用空间（这点跟NVMe把SQ/CQ都放在主机端变化挺大的，有点Host Base → Controller Base的意思）。

一次IO的传输过程如图6-66所示。

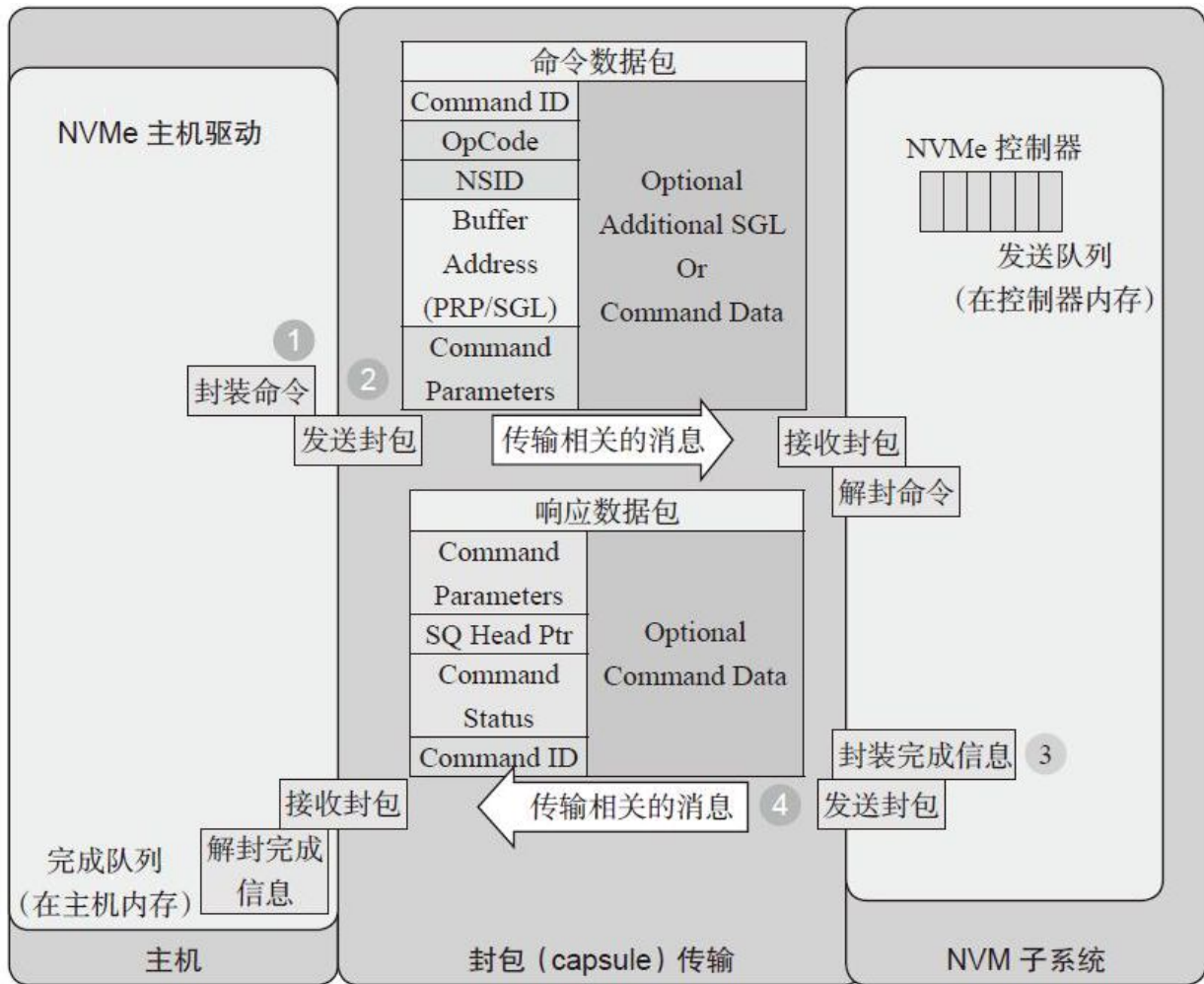


图6-66 NVMe Fabric IO传输流程示意图

- 1) 发送端 (Initiator) 驱动程序封装发送请求并派发给硬件。
- 2) 发送端硬件将发送请求发到目标端 (Target) 的发送队列。
- 3) 目标端控制器处理完成IO请求，并准备出来完成请求派发给硬件。
- 4) 目标端硬件将完成请求发到发送端的接收队列。

由于发送请求和完成请求可以直接携带数据，从而降低了互联中消耗的交互时间。

如果不需要在请求中携带数据，也可以由目标端在过程中直接从发起端获得相应的数据，如图6-67所示。

通过上述机制，NVMe over Fabrics协议实现了对于NVMe协议的命令和数据传输的扩展。

普通的NVMe命令都可以通过这套机制映射，NVMe的标准命令摇身一变，就成为互联协议的命令。

不过还是有一些场景是需要特殊考虑的，为了支持这些场景，协议扩展了NVMe命令，增加了与互联相关的5个命令：Connect、Property Get/Set、Authentication Send/Receive。

下面重点说一说Connect和Property Get/Set。

在NVMe over Fabrics协议中，约定每个发送队列都与一个接收队列一一对应，不允许多个发送队列使用同一个接收队列。发送接收队列对是通过Connect命令来创建的。Connect命令携带Host NQN、NVM Subsystem NQN和Host Identifier信息，并且可以指定连接到一个静态的控制器，或者连接到一个动态的控制器。一个主机可以通过不同的Host NQN或不同的Fabric端口（Port）建立到一个NVM Subsystem的多重连接。这种灵活性赋予了NVMe over Fabrics极大的灵活性。

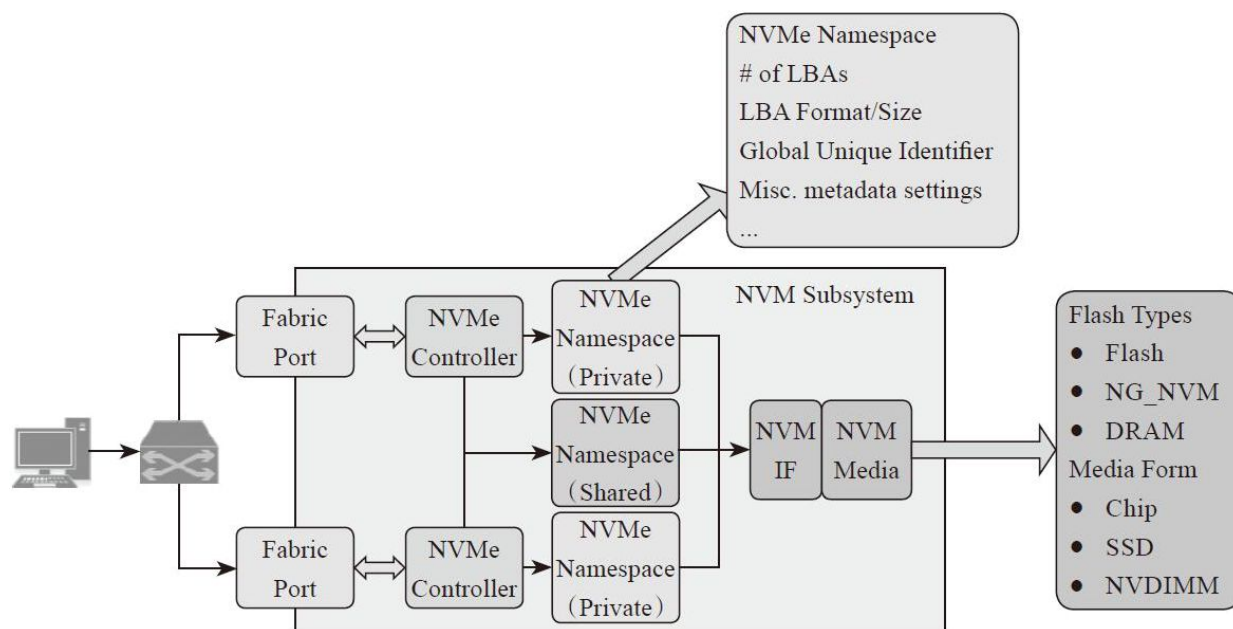


图6-67 目标端直接从发起端获得数据

在NVMe协议中，控制器是一个代表与主机进行沟通的接口实体。由于PCIe协议是一种树状拓扑结构，因此一旦控制器所处的PCIe端口定下来后，接口所关联的控制器就完全定下来了。而对于NVMe over Fabrics协议来说，一个Fabric的端口可以嵌入多个控制器，因此根据需要不同，可以选择实现静态控制器或动态控制器。动态控制器是一种简单的模型，适用于对主机具有相同服务特性的需求。静态控制器则适用于有不同需要的场景，发起者（Initiator）可以查询了解一个Fabric端口内部包含的静态控制器各自的能力，然后选择连接到指定的控制器以满足自身的需求。

在NVMe协议中，PCIe空间的BAR0（BAR1）描述了一段内存空间用于对控制器进行基本的寄存器级别的配置。由于Fabrics结构没有对应的实现，因此NVMe over Fabrics协议定义了Property Get/Set分别表示对控制器端寄存器的读取和写入动作。

至此，NVMe的标准操作就完全被准确和高效地映射成互连网络所对应的使用方式了。为了能满足互连网络的发现机制，NVMe over Fabrics协议定义了发现服务，用于让发起者主动发现NVM子系统和对应的可访问的Namespace。这个服务还同时用于支持多路径功能。该功能依赖于一个特殊的配置成支持发现服务的NVM子系统。发起者可以连接到该服务器并使用Discovery Log Page命令来获取可用的资源。

如表6-6所示，可以看出NVMe和NVMe over Fabrics的不同实现方式。

表6-6 NVMe与NVMe Over Fabrics的区别

区别	PCIe	Over Fabric
标识符	Bus/Device/Function	NVMe Qualified Name (NQN)
发现机制	总线枚举	通过 Discovery and Connect 命令
队列	基于内存	基于消息
数据传输方式	PRP 或 SGL	仅支持 SGL
发送队列和完成队列对应关系	一对一或者多对一	一对一
元数据存放	和块数据连续存放或者单独存放	和块数据连续存放
是否支持控制器向主机产生中断	支持	不支持

NVMe官网地址：<http://www.NVMexpress.org/>。

第7章 SSD测试

本章将介绍常用的SSD测试软件、研发过程中的测试流程、常用仪器设备及测试方法等。

7.1 主流SSD测试软件介绍

7.1.1 SSD性能测试第一神器——FIO

对于SSD性能测试来说，最好的工具莫过于FIO了。

图7-1中所示的这个可爱的小伙子名字叫Jens Axboe，他是丹麦哥本哈根大学计算机系没毕业的学生，他还有一个有名的同乡叫Linus，没想到老乡后来成了他的领导。Jens今年（2018年）41岁，16岁开始就接触Linux，后来也成了Linux开发者，现在是Linux Kernel大拿了，负责块设备层的维护。这个块设备层就是跟我们SSD关系最紧密的层级，联系了上层文件系统和下层设备驱动程序。他开发了不少有用的程序，比如Linux IO Scheduler里面的Deadline、CFQ Scheduler，还有著名的王牌测试工具FIO。Jens曾经在Fusion-IO、Oracle等工作，现在在Facebook。阿呆听说硅谷的Facebook给码农的薪水是最高的。



图7-1 FIO作者Jens

FIO是Jens开发的一个开源测试工具，功能非常强大，本节就只介绍其中一些基本功能：线程、队列深度、Offset、同步异步、DirectIO、BIO。

使用FIO之前，首先要有一些SSD性能测试方面的基础知识。

线程 指的是同时有多少个读或写任务在并行执行，一般来说，CPU里面的一个核心同一时间只能运行一个线程。如果只有一个核心，要想运行多线程，只能使用时间切片，每个线程跑一段时间片，

所有线程轮流使用这个核心。Linux使用Jiffies来代表一秒钟被划分成了多少个时间片，一般来说Jiffies是1000或100，所以时间片就是1毫秒或10毫秒。

一般电脑发送一个读写命令到SSD只需要几微秒，但是SSD要花几百微秒甚至几毫秒才能执行完这个命令。如果发一个读写命令，然后线程一直休眠，等待结果回来才唤醒处理结果，这叫作同步模式。可以想象，同步模式是很浪费SSD性能的，因为SSD里面有很多并行单元，比如一般企业级SSD内部有8~16个数据通道，每个通道内部有4~16个并行逻辑单元（LUN，Plane），所以同一时间可以执行32~256个读写命令。同步模式就意味着，只有其中一个并行单元在工作，暴殄天物。

为了提高并行性，大部分情况下SSD读写采用的是异步模式。就是用几微秒发送命令，发完线程不会傻傻地在那里等，而是继续发后面的命令。如果前面的命令执行完了，SSD通知会通过中断或者轮询等方式告诉CPU，由CPU来调用该命令的回调函数来处理结果。这样的好处是，SSD里面几十上百个并行单元都能分到活干，效率暴增。

不过，在异步模式下，CPU不能一直无限地发命令到SSD。比如SSD执行读写如果发生了卡顿，那有可能系统会一直不停地发命令，几千个，甚至几万个，这样一方面SSD扛不住，另一方面这么多命令会很占内存，系统也要挂掉了。这样，就带来一个参数叫作队列深度。举个例子，队列深度64就是说，系统发的命令都发到一个大小为64的队列，如果填满了就不能再发。等前面的读写命令执行完了，队列里面空出位置来，才能继续填命令。

一个SSD或者文件有大小，测试读写的时候设置Offset就可以从某个偏移地址开始测试。比如从offset=4G的偏移地址开始。

Linux读写的时候，内核维护了缓存，数据先写到缓存，然后再后台写到SSD。读的时候也优先读缓存里的数据。这样速度可以加快，但是一旦掉电，缓存里的数据就没了。所以有一种模式叫作DirectIO，跳过缓存，直接读写SSD。

Linux读写SSD等块设备使用的是BIO（Block-IO），这是个数据结构，包含了数据块的逻辑地址LBA，数据大小和内存地址等。

1.FIO初体验

一般Linux系统是自带FIO的，如果没有或者版本太老，要自己从<https://github.com/axboe/fio> 下载最新版本源代码编译安装。进入代码主目录，输入下列命令就编译安装好了。

```
./configure;make && make install
```

帮助文档用下面命令查看：

```
man fio
```

先来看一个简单的例子：

```
fio -rw=randwrite -ioengine=libaio -direct=1 -thread-numjobs=1 -iodepth=64 -  
filename=/dev/sdb4 -size=10G -name=job1 -offset=0MB -bs=4k -name=job2 -  
offset=10G -bs=512 --output TestResult.log
```

每一项的意思都可以从fio帮助文档查到，这里的参数解释如下：

·fio：软件名称。

·-rw=randwrite：读写模式，randwrite是随机写测试，还有顺序读read，顺序写write，随机读randread，混合读写等。

·-ioengine=libaio：libaio指的是异步模式，如果是同步就要用sync。

·-direct=1：是否使用directIO。

·-thread：使用pthread_create创建线程，另一种是fork创建进程。进程的开销比线程要大，一般都采用thread测试。

·-numjobs=1：每个job是1个线程，这里用了几，后面每个用-name指定的任务就开几个线程测试。所以最终线程数=任务数×numjobs。

·-iodepth=64：队列深度64。

·-filename=/dev/sdb4: 数据写到/dev/sdb4这个盘（块设备）。这里可以是一个文件名，也可以是分区或者SSD。

·-size=10G: 每个线程写入数据量是10GB。

·-name=job1: 一个任务的名字，名字随便起，重复了也没关系。这个例子指定了job1和job2，建立了两个任务，共享-name=job1之前的参数。-name之后的就是这个任务独有的参数。

·-offset=0MB: 从偏移地址0MB开始写。

·-bs=4k: 每一个BIO命令包含的数据大小是4KB。一般4kB IOPS测试，就是在这里设置。

·--output TestResult.log: 日志输出到TestResult.log。

2.FIO结果解析

我们来看一个FIO测试随机读的结果。命令如下，两个任务并行测试，队列深度64，异步模式，每个任务测试数据1GB，每个数据块4KB。所以，这个命令是在测试两个线程、队列深度64下的4kB随机读IOPS。

```
# fio -rw=randread -ioengine=libaio -direct=1 -iodepth=64 -filename=/dev/sdc -
size=1G -bs=4k -name=job1 -offset=0G -name=job2 -offset=10G
job1: (g=0): rw=randread, bs=4K-4K/4K-4K/4K-4K, ioengine=libaio, iodepth=64
job2: (g=0): rw=randread, bs=4K-4K/4K-4K/4K-4K, ioengine=libaio, iodepth=64
fio-2.13
Starting 2 processes
Jobs: 2 (f=2)
job1: (groupid=0, jobs=1): err= 0: pid=27752: Fri Jul 28 14:16:50 2017
read : io=1024.0MB, bw=392284KB/s, iops=98071, runt= 2673msec
slat (usec): min=6, max=79, avg= 9.05, stdev= 2.04
clat (usec): min=148, max=1371, avg=642.89, stdev=95.08
lat (usec): min=157, max=1380, avg=651.94, stdev=95.16
clat percentiles (usec):
|  1.00th=[ 438],  5.00th=[ 486], 10.00th=[ 516], 20.00th=[ 564],
| 30.00th=[ 596], 40.00th=[ 620], 50.00th=[ 644], 60.00th=[ 668],
| 70.00th=[ 692], 80.00th=[ 724], 90.00th=[ 756], 95.00th=[ 796],
| 99.00th=[ 884], 99.50th=[ 924], 99.90th=[ 1004], 99.95th=[ 1048],
| 99.99th=[ 1144]
lat (usec) : 250=0.01%, 500=6.82%, 750=81.14%, 1000=11.93%
lat (msec) : 2=0.11%
cpu           : usr=9.09%, sys=90.08%, ctx=304, majf=0, minf=98
IO depths    : 1=0.1%, 2=0.1%, 4=0.1%, 8=0.1%, 16=0.1%, 32=0.1%, >=64=100.0%
submit      : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%,
>=64=0.0%
```

```

        complete : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.1%,
>=64=0.0%
        issued   : total=r=262144/w=0/d=0, short=r=0/w=0/d=0, drop=r=0/w=0/d=0
        latency   : target=0, window=0, percentile=100.00%, depth=64
job2: (groupid=0, jobs=1): err= 0: pid=27753: Fri Jul 28 14:16:50 2017
read : io=1024.0MB, bw=447918KB/s, iops=111979, runt= 2341msec
slat (usec): min=5, max=41, avg= 6.30, stdev= 0.79
clat (usec): min=153, max=1324, avg=564.61, stdev=100.40
lat (usec): min=159, max=1331, avg=570.90, stdev=100.41
clat percentiles (usec):
| 1.00th=[ 354], 5.00th=[ 398], 10.00th=[ 430], 20.00th=[ 474],
| 30.00th=[ 510], 40.00th=[ 540], 50.00th=[ 572], 60.00th=[ 596],
| 70.00th=[ 620], 80.00th=[ 644], 90.00th=[ 684], 95.00th=[ 724],
| 99.00th=[ 804], 99.50th=[ 844], 99.90th=[ 932], 99.95th=[ 972],
| 99.99th=[ 1096]
lat (usec) : 250=0.03%, 500=27.57%, 750=69.57%, 1000=2.79%
lat (msec) : 2=0.04%
cpu        : usr=11.62%, sys=75.60%, ctx=35363, majf=0, minf=99
IO depths  : 1=0.1%, 2=0.1%, 4=0.1%, 8=0.1%, 16=0.1%, 32=0.1%, >=64=100.0%
submit     : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%,
>=64=0.0%
        complete : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.1%,
>=64=0.0%
        issued   : total=r=262144/w=0/d=0, short=r=0/w=0/d=0, drop=r=0/w=0/d=0
        latency   : target=0, window=0, percentile=100.00%, depth=64

Run status group 0 (all jobs):
      READ: io=2048.0MB, aggrb=784568KB/s, minb=392284KB/s, maxb=447917KB/s,
      mint=2341msec, maxt=2673msec

Disk stats (read/write):
      sdc: ios=521225/0, merge=0/0, ticks=277357/0, in_queue=18446744073705613924,
      util=100.00%

```

FIO会为每个Job打印统计信息。最后面是合计的数值。我们一般看重的是总的性能和延迟。

首先看的是最后总的**带宽**，aggrb=784568KB/s，算成4KB就是196k **IOPS**。

再来看看**延迟（Latency）**。Slat是发命令时间，slat（usec）：min=6，max=79，avg=9.05，stdev=2.04说明最短时间6微秒，最长79微秒，平均9微秒，标准差2.04。clat是命令执行时间，lat就是总的延迟。看得出来，读的平均延迟在571微秒左右。

clat percentiles（usec）给出了延迟的统计分布。比如90.00th=[684]说明90%的读命令延迟都在684微秒以内。

3.用FIO做数据校验

用FIO可以检验写入数据是否出错。用-verify=str来选择校验算法，有md5、crc16、crc32、crc32c、crc32c-intel、crc64、crc7、sha256、sha512、sha1等。为了校验，需要用do_verify参数。如果是写，那么do_verify=1就意味着写完再读校验，这种会很占内存，因为FIO会把每个数据块的校验数据保存在内存里。do_verify=0时只写校验数据，不做读校验。

读的时候如果do_verify=1，那么读出来的数据都会做校验值检查；如果do_verify=0，则只读数据，不做检查。

另外，verify=meta时，fio会在数据块内写入时间戳、逻辑地址等，此时还能用verify_pattern指定写入数据pattern。

4.FIO其他功能

FIO功能非常强大，可以通过man来查看每一个功能，也有网页版帮助文档<https://linux.die.net/man/1/fio>。

5.FIO配置文件

前面的例子都是用命令行来测试，其实也可以用配置文件把这些参数写进去。比如新建FIO配置文件test.log内容如下：

```
[global]
filename=/dev/sdc
direct=1
iodepth=64
thread
rw=randread
ioengine=libaio
bs=4k
numjobs=1
size=10G

[job1]
name=job1
offset=0

[job2]
name=job2
offset=10G

;--end job file
```

保存后，只需要fio test.log就能执行测试任务了，是不是很方便？

7.1.2 AS SSD Benchmark

AS SSD Benchmark是一款来自德国的SSD专用测试软件，可以测试连续读写、4K对齐、4KB随机读写和响应时间的表现，并给出一个综合评分。它有两种模式可选，即MB/s与IOPS，如图7-2所示。

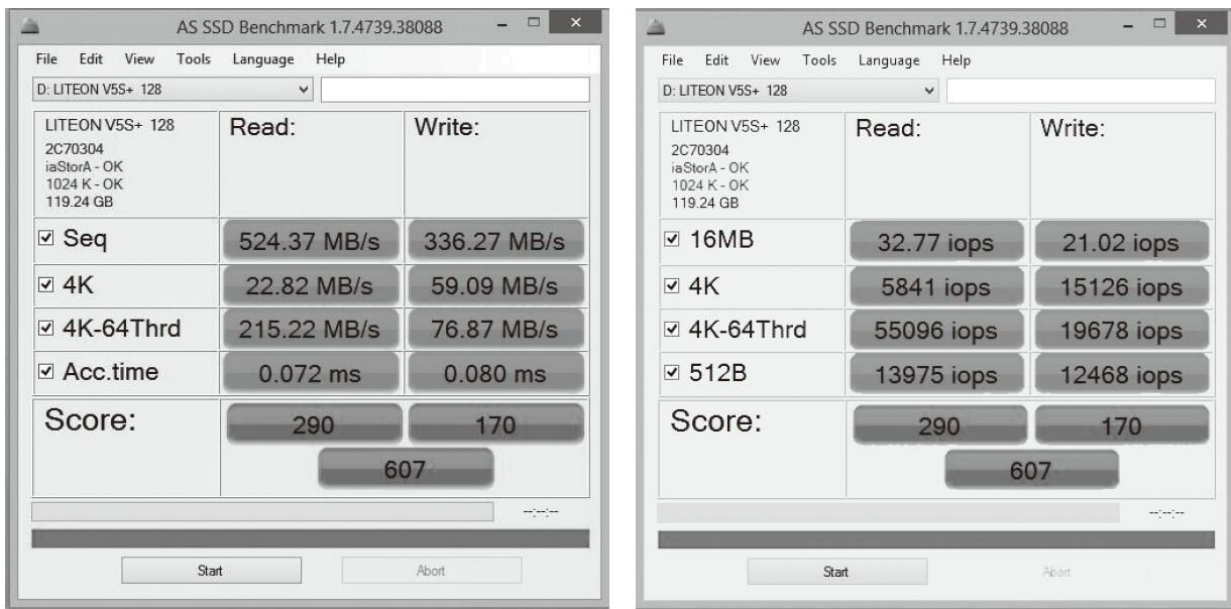


图7-2 AS SSD Benchmark测试指标

AS SSD Benchmark在测试时一共会生成和写入5GB的测试数据文件，所有3个测试传输率项目都是去读写这些数据文件来换算速度的。其4KB QD64主要是用来测NCQ（Native Command Queuing，原生命令队列）差距的。IDE模式下就和普通4KB随机没有任何区别。由于每个测试都需要进行一定大小的数据读写，硬盘性能越低，测试需要花费的时间就越久，拿机械硬盘来跑这个测试并不适宜，跑完全程大约需要1个小时左右。寻址时间测试，读取是测试寻址随机的4KB文件（全盘LBA区域），写入是测试寻址随机的512B文件（指定的1GB地址范围）。注意，运行AS SSD基准测试至少需要2GB的空闲空间。

AS SSD Benchmark除了可以测试SSD的性能外，还可以检测出SSD的固件算法、是否打开AHCI模式、是否进行4K对齐等（见图7-3），是目前应用十分广泛的SSD测试软件。



图7-3 AS SSD Benchmark测试对象信息

AS SSD Benchmark使用的测试数据是随机的。

7.1.3 ATTO Disk Benchmark

ATTO Disk Benchmark是一款简单易用的磁盘传输速率检测软件，可以用来检测硬盘、U盘、存储卡及其他可移动磁盘的读取及写入速率。该软件使用了不同大小的数据测试包，数据包按512B、1K、2K直到8K进行读写测试，测试完成后数据用柱状图的形式表达出来，体现文件大小比例不同对磁盘速度的影响。

ATTO测试是极限情况下的磁盘持续读写性能，采用的测试模型具有很高的可压缩性。[ATTO默认测试全0数据](#)。它的应用截图如图7-4所示。

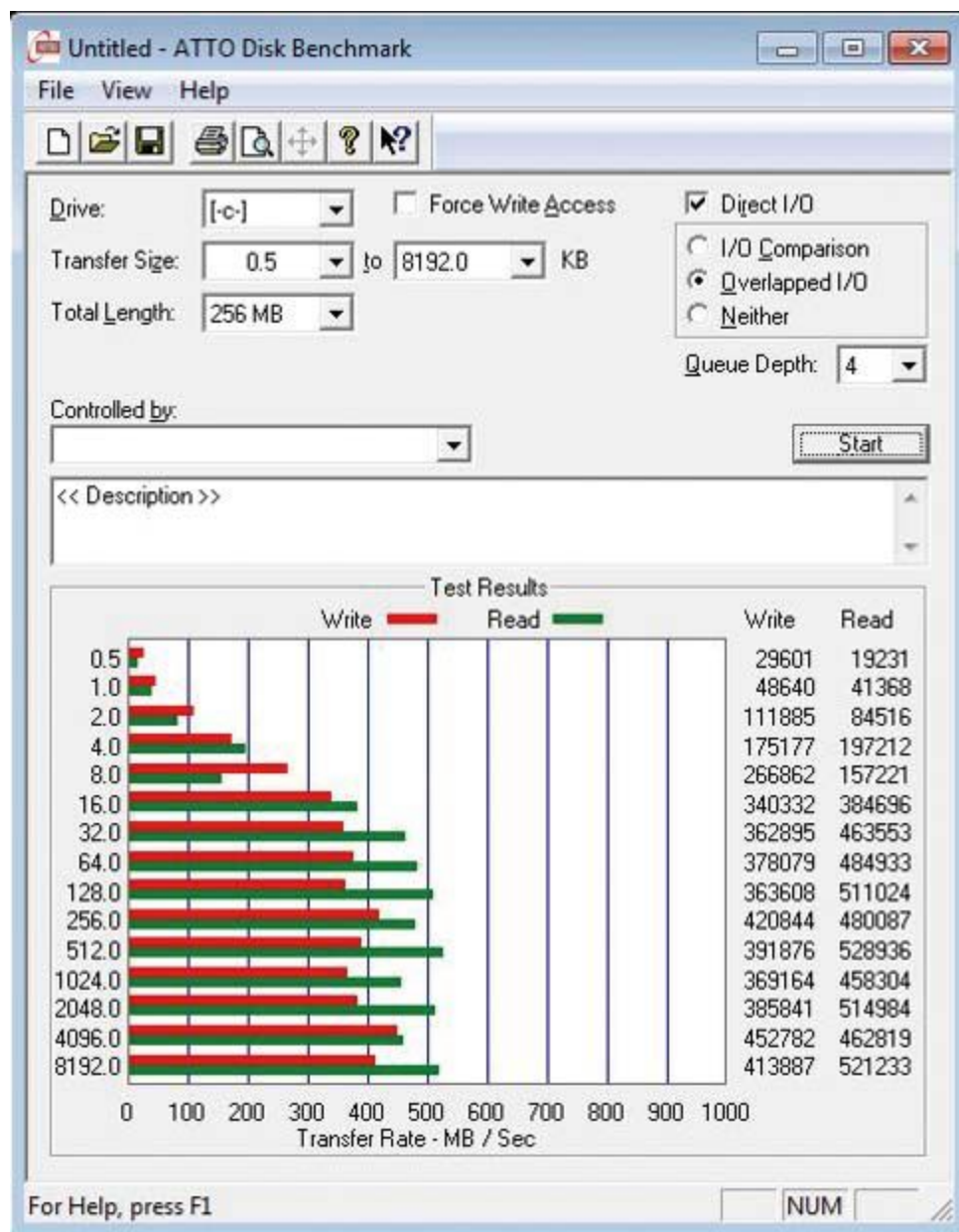


图7-4 ATTO应用截图

7.1.4 CrystalDiskMark

CrystalDiskMark软件是一个测试硬盘或者存储设备的小巧工具，测试存储设备大小和测试次数都可以选择。测试项目里分为，持续传输率测试（块单位1024KB），随机512KB传输率测试，随机4KB测试，随机4KB QD32（队列深度32）测试，如图7-5所示。

CrystalDiskMark默认运行5次，每次100MB的数据量，取最好成绩。

CrystalDiskMark软件测试前，同样会生成一个测试文件（大小由用户自行设置）。一般来说，设置得越大，数据缓存的干扰越少，成绩就更能反映SSD的真实性能，不过缺点是会影响SSD的耐久度（写入太多数据影响P/E）。所以一般测试时都采纳软件默认值。

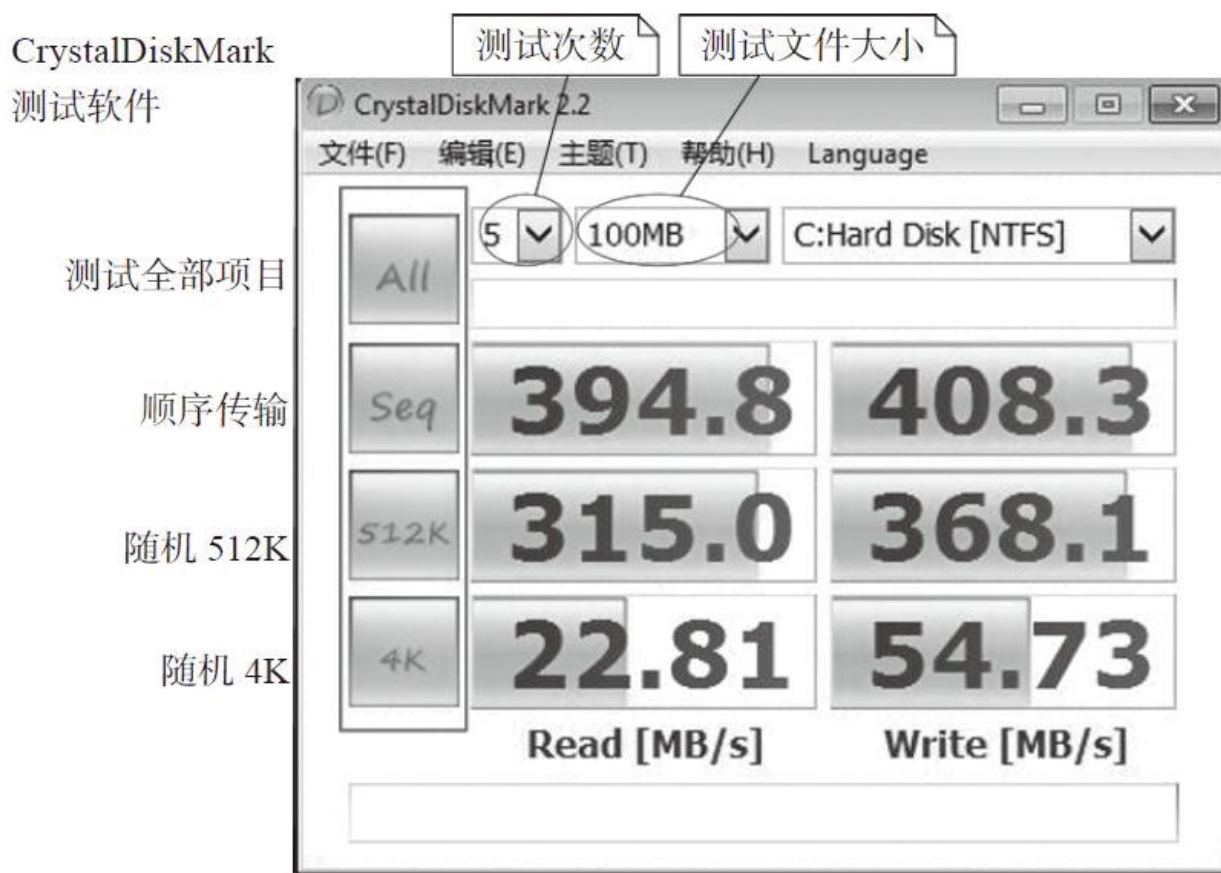
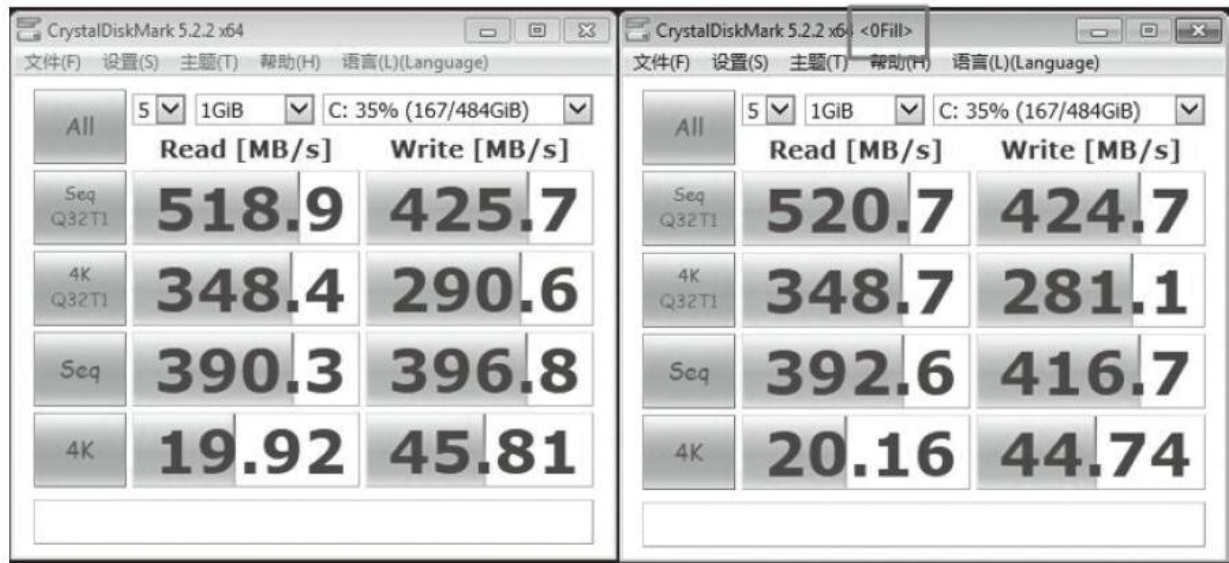


图7-5 CrystalDiskMark测试指标

软件默认测试数据为不可压缩数据。如果设置选项中选择了<All 0x00, 0Fill>或<All 1x00.1Fill>，测试成绩会大不一样。其实就是把数

据模型改为全部是可压缩连续数据，这跟ATTO测试原理一样，测试出来成绩相当不错，但实际参考意义并不大。修改数据模型后有一个明显的特征，CDM的标题栏上会直接标注出来，如图7-6所示。



将软件设置成，<All，0x0 Fill> 或者 <All 0x0 Fill>，其实就是把数据模型改成全部是 0 或 1 可压缩连续数据。

图7-6 CrystalDiskMark设置不同填充Pattern

7.1.5 PCMark Vantage

PCMark Vantage可以衡量各种类型PC的综合性能。从多媒体家庭娱乐系统到笔记本，从专业工作站到高端游戏平台，无论是专业人士还是普通用户，都能通过PCMark Vantage透彻了解其性能，从而发挥最大性能。测试内容可以分为以下三个部分：

1) 处理器测试：基于数据加密、解密、压缩、解压缩、图形处理、音频和视频转码、文本编辑、网页渲染、邮件功能、处理器人工智能游戏测试、联系人创建与搜索。

2) 图形测试：基于高清视频播放、显卡图形处理、游戏测试。

3) 硬盘测试：使用Windows Defender、《Alan Wake》游戏、图像导入、Windows Vista启动、视频编辑、媒体中心使用、Windows Media Player搜索和归类，以及某些程序的启动（如Office Word 2007、Adobe Photoshop CS2、Internet Explorer、Outlook 2007）。

7.1.6 IOMeter

IOMeter是一个单机或者集群的I/O子系统测量和描述工具。与前面介绍的测试软件相比，IOMeter在测试软件中是属于比较自由的，用户可以按照测试需求去配置测试磁盘数据范围、队列深度、数据模式（可压缩或者不可压缩，有些版本支持，有些老版本不支持）、测试模式（随机或者顺序访问）、读写测试比例、随机和顺序访问比例，以及测试时间等。IOMeter应用截图如图7-7所示。

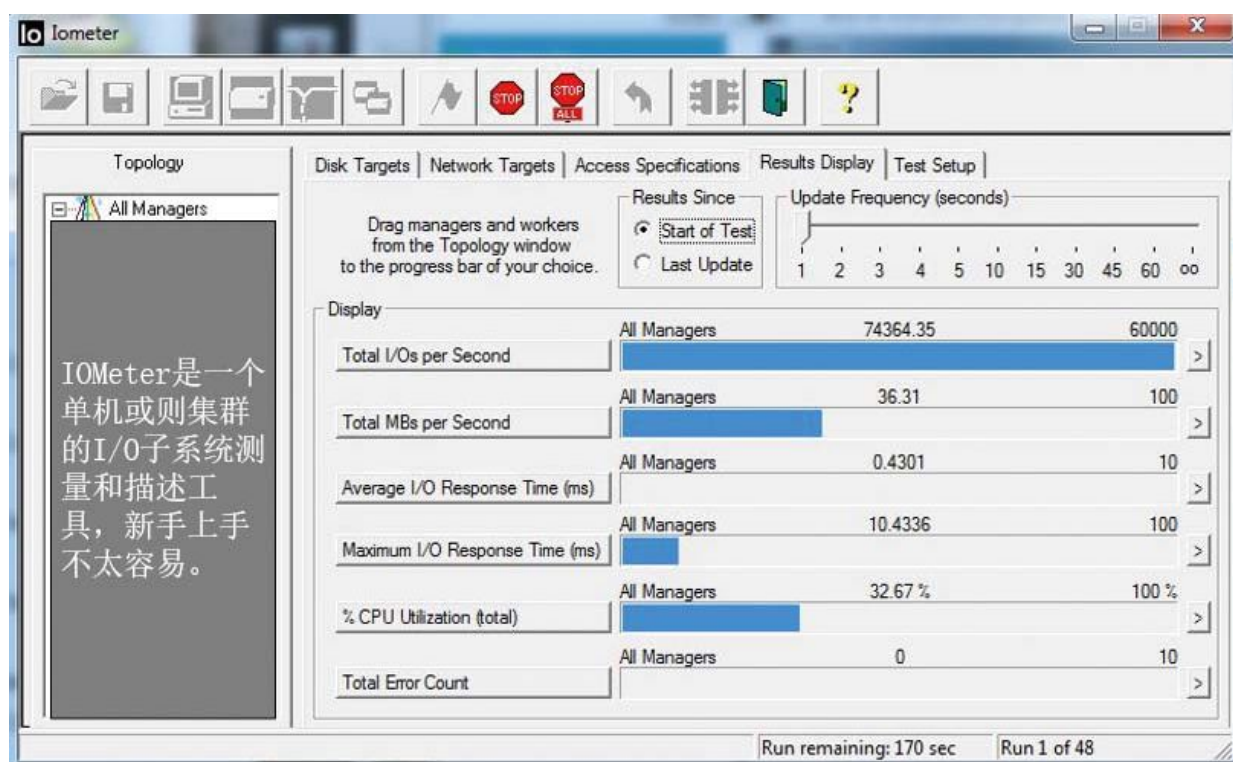


图7-7 IOMeter应用截图

本地IO性能测试:

- 1) 启动程序，在Windows上单击IOMeter图标；
- 2) 在Disk Targets页中选择一个驱动器；
- 3) 在Access Specifications页中选择一个需要的测试项目；

4) 在Results Display页中设置Update Frequency (Seconds)，即设置多长时间统计一次测试结果，如果不设置，不但在测试期间不显示测试结果，而且在测试结束后在测试结果文件中也没有数据；

- Total I/Os per Second: 数据存取速度，该值越大越好；

- Total MBs per Second: 数据传输速度，该值越大越好；

- Average I/O Response Time: 平均响应时间，该值越小越好；

- CPU Utilization: CPU占用率，越低越好；

5) 单击工具栏中的Start Tests按钮，选择一个测试结果输出文件后开始一个测试（一般一次测试运行10分钟即可）；

6) 测试完成后单击“stop”按钮停止所有测试；

7) 查看测试结果，由于IOMeter没有提供一个GUI的查看测试报告的工具。可以使用Excel打开测试结果文件“csv”，然后利用Excel的图标工具整理测试结果。或者使用IOMeter提供“Import Wizard for MS Access”将测试结果导入一个Access文件。

7.2 验证与确认

SSD从设计、固件到成品出货，少不了各种测试。中文博大精深，将这些都叫测试，到英文里则会对应N个词：Simulation、Emulation、Verification、Validation、Test、QA。

先聊一下Verification和Validation。

为了帮助理解，先简单说一下芯片设计的过程：

- 1) 需求：老大们商量这颗主控要实现什么功能。
- 2) 架构：Architecture出设计图。
- 3) 设计：ASIC把各种内部、外部IP攒起来。
- 4) TapeOut。
- 5) 芯片回来。

在设计阶段，使用Emulator（以后介绍）或者FPGA进行测试的过程，叫Verification，中文翻译为“验证”——目的是为了帮助ASIC把事情做对。

在芯片回来以后，使用开发板进行测试的过程，叫Validation，中文翻译为“确认”——目的是确保ASIC把事情给做对了。

在Verification阶段，一旦发现问题，ASIC工程师可以马上fix，然后通过升级Emulator的database或者更新FPGA的bit file把新的RTL交给测试再验证一遍，一直到做对为止。

相同的问题，如果是Validation阶段才发现，则只能通过重新TapeOut（含mental fix）或者让固件“打掩护”了。

7.3 测试仪器

7.3.1 Emulator

在SSD主控芯片设计阶段，除了RTL Simulation以外，通常还会进行Verification的工作，而Verification中就会使用到Emulator或者FPGA。

先说一下Simulation和Emulation的区别：

- Simulator**是做仿真，基于软件，重点是实现芯片的功能并输出结果；

- Emulator**是做模拟，用硬件实现，通过模拟实现芯片的内部设计，从而实现功能并输出结果。

图7-8为业界比较知名的Emulator提供商Cadence旗下的Emulator产品Palladium系列。



图7-8 Emulator

按照官方的说法，它可以做Simulation、Simulation Acceleration和Emulation。

在设计SSD主控芯片时，Emulator和FPGA都可以用于ASIC Verification，那这两者区别有哪些？个人理解，主要有这么几点：

1) 价格：Emulator大概百万美元级别，FPGA大概是数千到万美元级别；

2) 能力：Emulator的逻辑可以到23亿门（这是老款Palladium XP，最新款据Palladium Z1达到了90亿门），FPGA大概是百万门级别。对应到SSD主控里，一块FPGA可能只能模拟前段（PCIe+NVMe），后端（闪存Controller）可能需要另外一块FPGA，而Emulator，只要你想塞，整个ASIC的RTL塞进去也是妥妥的；

3) Debug：Emulator可以比较方便地导出ASIC工程师所需要的信号并抓取硬件逻辑波形，而FPGA在连接协议分析仪、逻辑分析仪方面比较方便；

4) 速度：Emulator虽然好，但是速度比FPGA要慢得多——来个传说中的例子：如果FPGA上boot一个OS要几个小时，那Emulator上boot一个OS可能要几天；

5) 档次：FPGA是个公司就能有，Emulator则绝对是实力的彰显——有领导、VIP来参观的时候，给参观一下，顿时就跟其他公司拉开差距了；

归根结底，Emulator和FPGA都是很好的工具，需要正确、合理地使用，才能更好地在芯片研发阶段发现更多ASIC问题。

Emulator（或FPGA）的另一个好处是，固件团队可以使用这些工具提前开始开发，不用等芯片回来以后，先经历“不死也要脱层皮”的Bringup阶段，然后才开始“遇到问题不知道硬件原因还是代码原因的”开发阶段。

Emulator——致力于构建SSD主控和谐团队！

7.3.2 协议分析仪

要测试SSD，需要很多很多不一样的设备，需要花很多很多的银子。

目前市面上的SSD接口挺多，如SATA、SAS、PCIe、U.2、M.2、MSATA、GumStick，

其实走的前端协议就两大类：SATA/SAS和PCIe。

一颗SSD主控一般分前、中、后三段，前端就是SATA/SAS和PCIe这些配上AHCI或者NVMe，中段就是FTL，后端就是闪存控制器。

FTL是纯软件实现，测这个基本上不需要什么设备。

后端跟闪存打交道，主要用逻辑分析仪，另一种巨贵的仪器，这里不展开说。

这里先聊两种协议分析仪（Analyzer），SATA/SAS Analyzer和PCIe Analyzer。

Analyzer是什么？你可以这么理解，以SATA Analyzer为例，SATA Host和SATA SSD之间传输命令和数据，就像两个人在打电话，不在这个线路上的你，正常情况下是听不到他们说了什么的。但通过Analyzer，你就可以完完整整地知道他们之间的对话，同时还不会让他们俩察觉。

SATA/SAS Analyzer的供应商，平时接触比较多的有两家：SerialTek和LeCroy。

如图7-9所示为SerialTek SATA/SAS Analyzer。



图7-9 SerialTek SATA/SAS协议分析仪

连在主机和SSD之间的示意图如图7-10所示。

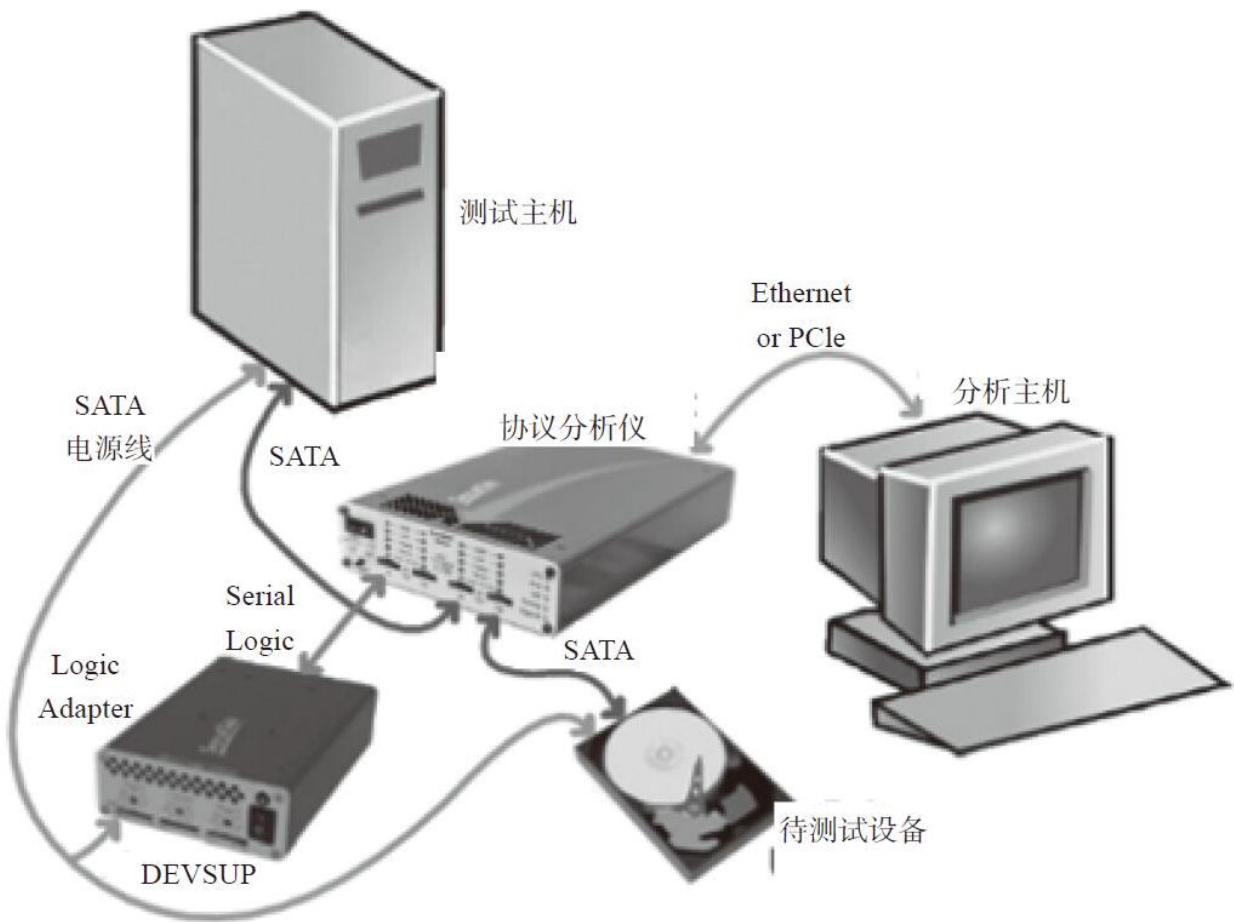


图7-10 SATA协议分析仪连接示意图

抓到的Trace是这个样子，如图7-11所示。

Time	Delta time	Channel	Type - Initiator	Type - Target	Decode	Command
0.002.344.706	5,642	14	DATA		ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.349.632	4,926	T4		DMA Setup (FIS 41)	STP DMA SETUP (FIS 41); D:0; I:0; A:0; Offset:0h; 512 bytes	
0.002.373.930	24,290	T4		OPEN	ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.377.598	3,668	T4		DMA Activate (FIS 39)	STP DMA ACTIVATE (FIS 39)	
0.002.387.166	9,568	14	Data (FIS 46)		STP DATA (FIS 46); 512 bytes	
0.002.397.592	10,426	14	OPEN		ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.401.796	4,206	14	Register Host->Dev (FIS 27)		STP REGISTER HOST->DEV (FIS 27); WRITE FPDMA QUEUED	61: WRITE FPDMA QUEUED
0.002.450.036	48,238	T4		OPEN	ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.453.810	3,774	T4		Register Dev->Host (FIS 34)	STP REGISTER DEV->HOST (FIS 34); D:0; Status:40h; Error:00h	
0.002.459.050	5,240	T4		OPEN	ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.459.320	270	14	OPEN		ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.462.130	2,810	T4		Set Device Bits (FIS A1)	STP SET DEVICE BITS (FIS A1); Tags: 1 9 10; I:1; N:0; Status...	
0.002.468.922	6,792	14	Register Host->Dev (FIS 27)		STP REGISTER HOST->DEV (FIS 27); READ FPDMA QUEUED	60: READ FPDMA QUEUED
0.002.491.578	22,606	T4		OPEN	ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.495.222	3,694	T4		Register Dev->Host (FIS 34)	STP REGISTER DEV->HOST (FIS 34); D:0; Status:40h; Error:00h	
0.002.500.800	5,500	14	OPEN		ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.504.950	4,148	14	Register Host->Dev (FIS 27)		STP REGISTER HOST->DEV (FIS 27); READ FPDMA QUEUED	60: READ FPDMA QUEUED
0.002.518.514	31,564	T4		OPEN	ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.542.234	3,720	T4		Register Dev->Host (FIS 34)	STP REGISTER DEV->HOST (FIS 34); D:0; Status:40h; Error:00h	
0.002.547.756	5,524	14	OPEN		ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.551.970	4,212	14	Register Host->Dev (FIS 27)		STP REGISTER HOST->DEV (FIS 27); READ FPDMA QUEUED	60: READ FPDMA QUEUED
0.002.555.016	3,046	14	OPEN		ADDRESS OPEN; PROTOCOL:1(SSP); Rate:8(1,5 Gbps)	
0.002.556.274	1,258	14	COMMAND		SSP COMMAND: WRITE (10)	2a: WRITE (10)
0.002.569.980	13,700	T4		OPEN	ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.573.648	3,668	T4		Register Dev->Host (FIS 34)	STP REGISTER DEV->HOST (FIS 34); D:0; Status:40h; Error:00h	
0.002.578.758	5,110	T3		OPEN	ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.579.310	552	14	OPEN		ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.582.420	3,110	T4		DMA Setup (FIS 41)	STP DMA SETUP (FIS 41); D:1; I:0; A:0; Offset:0h; 512 bytes	
0.002.601.740	19,320	T4		OPEN	ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.605.486	3,746	14	Data (FIS 46)		STP DATA (FIS 46); 512 bytes	
0.002.616.094	10,608	14	Register Host->Dev (FIS 27)		STP REGISTER HOST->DEV (FIS 27); WRITE FPDMA QUEUED	61: WRITE FPDMA QUEUED
0.002.728.064	112,870	T4		OPEN	ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.732.658	3,694	T4		Register Dev->Host (FIS 34)	STP REGISTER DEV->HOST (FIS 34); D:0; Status:40h; Error:00h	
0.002.738.228	5,370	14	OPEN		ADDRESS OPEN; PROTOCOL:2(STP); Rate:8(1,5 Gbps)	
0.002.742.374	4,146	14	Register Host->Dev (FIS 27)		STP REGISTER HOST->DEV (FIS 27); WRITE FPDMA QUEUED	61: WRITE FPDMA QUEUED
0.002.745.514	3,140	14	OPEN		ADDRESS OPEN; PROTOCOL:1(SSP); Rate:8(1,5 Gbps)	

图7-11 SATA Trace示例

PCIe Analyzer的供应商主要有三家：LeCroy、SerialTek和Agilent。

如图7-12所示为LeCroy的PCIe Analyzer。



图7-12 LeCroy PCIe协议分析仪

它配有各种Interposer卡，如图7-13所示。

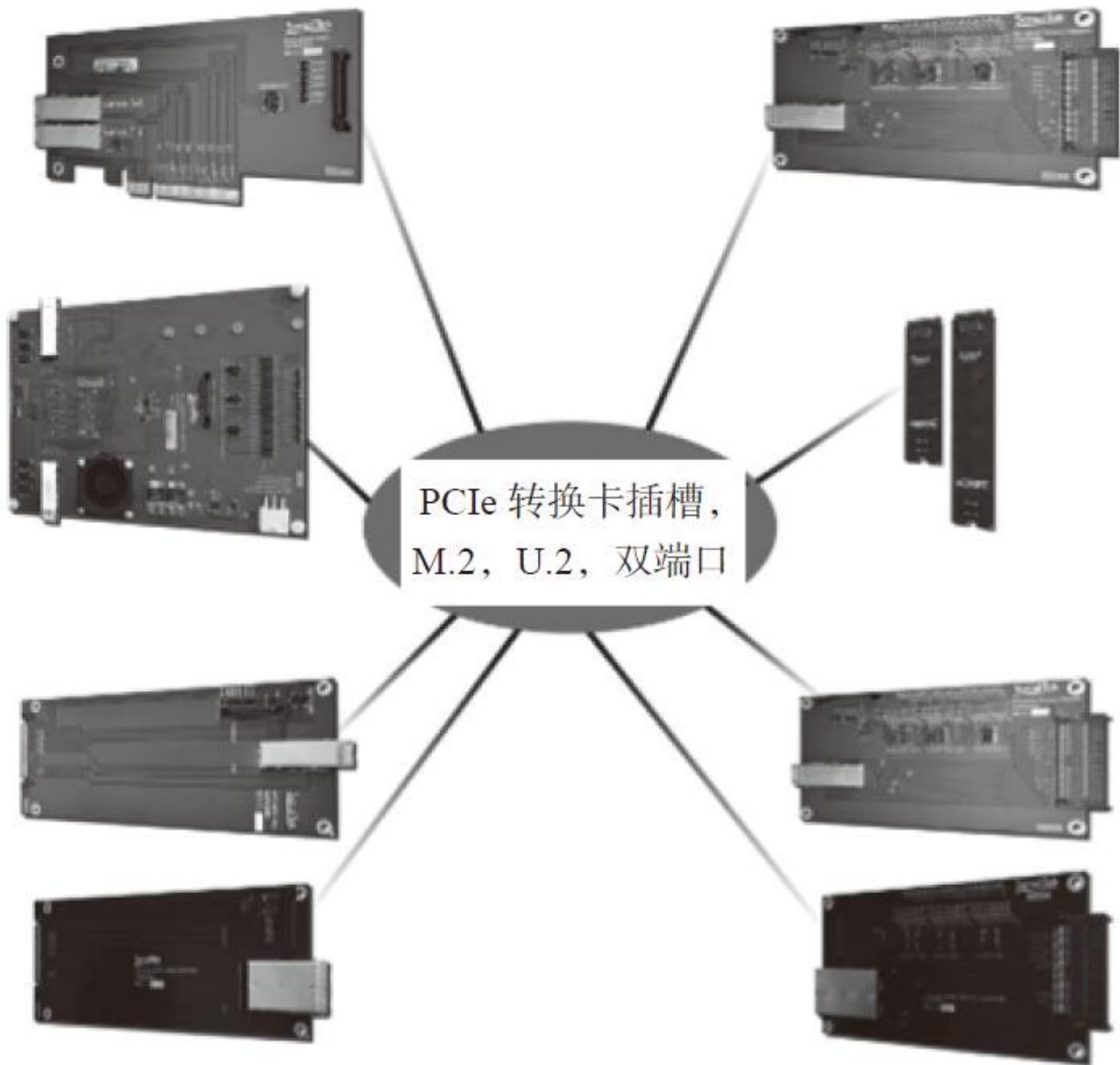


图7-13 LeCroy PCIe协议分析仪Interposer cards

抓到的Trace是这个样子的（这是一个NVMe读写的命令，LeCroy可以帮你解码NVMe、AHCI这种常见的存储协议），图7-14中，软件将PCIe Trace中的NVMe命令解析了出来。

使用PCIe Analyzer可以测量PCIe的物理层、链路层、事务层。跟示波器不同，Analyzer可以基于PCIe协议将链路上所有Lane上发生的事务都解析出来，并且还提供Trigger（触发）的功能。

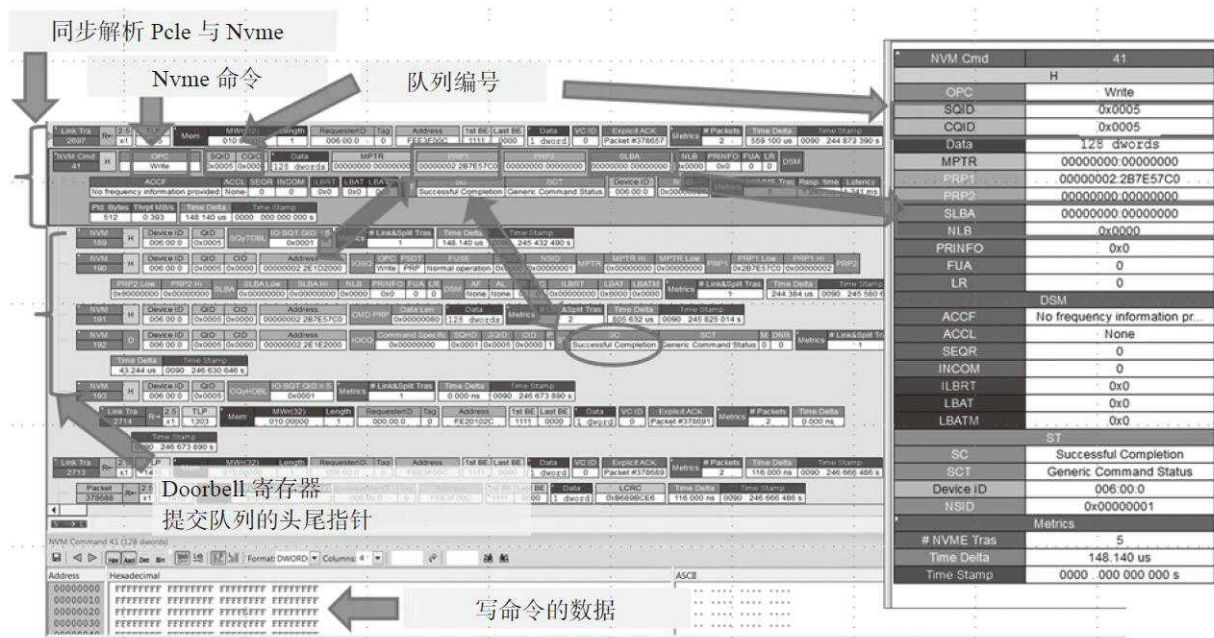


图7-14 PCIe软件解析NVMe指令

对于Analyzer的一大挑战就是在链路电源状态切换的过程能够快速适应，越早实现正确的抓包并解析越好。

这点在调试的时候尤其重要，看一个实际的例子：对一个寄存器做CfgWr操作，但是结果发现写进去的值不对，而且这个问题只在ASPM enable的时候才会发生。

电源状态切换对于PCIe发送端和接收端来说是属于压力比较大的操作，因此有时会导致链路不稳定从而发送错误的包。这种问题调试需要抓trace，而analyzer必须把在链路从L0s退出进入L0时所发送的全部TLP都抓到，否则就无法查看错误到底在什么地方。且L0s退出的时间非常短，所以Analyzer需要在链路从electrical idle（空闲状态）退出后非常短的时间内（几十个FTS [1]）就能正确抓包并解析。

工具是死的，人是活的，什么时候抓trace，抓哪个阶段，抓的时候满屏的红色怎么办，怎么设Trigger，trace怎么分析？这些就需要工程师们自己花时间琢磨了。

[1] 全称为Fast Training Sequence。

7.3.3 Jammer

再牛的肖邦，也弹不出SSD厂商的悲伤。

一块SSD到不同客户手上，不知道会接在什么机器，使用什么样的OS和主机驱动，在什么环境下使用。结合巨大的使用数量，不知道哪天某块SSD就会从主机那边收到一个不按套路出牌的FIS或者Primitive (SATA SSD)。

举个例子：主机发了一个读命令，SSD二话不说开始干活，辛辛苦苦把数据从闪存里读出来，仔仔细细地进行ECC解码，小心翼翼传到DDR，进行MPECC检查，再全神贯注地传到SATA模块的某个FIFO，这时候SSD抹抹头上的汗，把手擦干净，写了一张字条，上书“X_RDY”，恭恭敬敬地递给主机，然后把数据捧在怀里，细心地用SOF包装好，殷切地期盼主机也回复一张小字条“R_RDY”。主机十分感动地看着SSD，然后回复了一句“R_ERR”拒绝了它。

客户们的要求是一样的——“主机虐你千百遍，SSD你要待他如初恋”——术语叫作Robustness（健壮性）。

为了保证健壮性，ASIC和固件工程师们要花大量的精力，脑补各种错误可能性，在RTL和FW中加入相应的错误处理（Error Handling）的流程。

这么做有两个问题：这些错误处理的流程，在实验室里面跑一星期，可能都撞不到一个；再牛的工程师也没法提前考虑到各种错误。

与其让别人找麻烦，不如自己给自己找麻烦。搞测试的就是平时给ASIC和固件找麻烦，以SATA SSD为例，可以用一种工具——Jammer。

图7-15中所示小一号的那个就是SATA Jammer。



图7-15 SATA协议分析和Jammer

如果说Analyzer是一个“窃听器”，让你知道主机和设备之间发生了什么，那么Jammer就是一个“邮递员”，主机和设备之间所有的通信都必须经过它的手，然后Jammer可以把信拆开，将里面的内容修改或者替换，再转发出去。

结合之前的例子，我们可以把正常主机回复R_RDY改成R_ERR，从而检查SSD遇到这种情况时处理的是否正确。

图7-16所示为Jammer管理软件截图——向一个Data FIS中故意注入CRC Error。

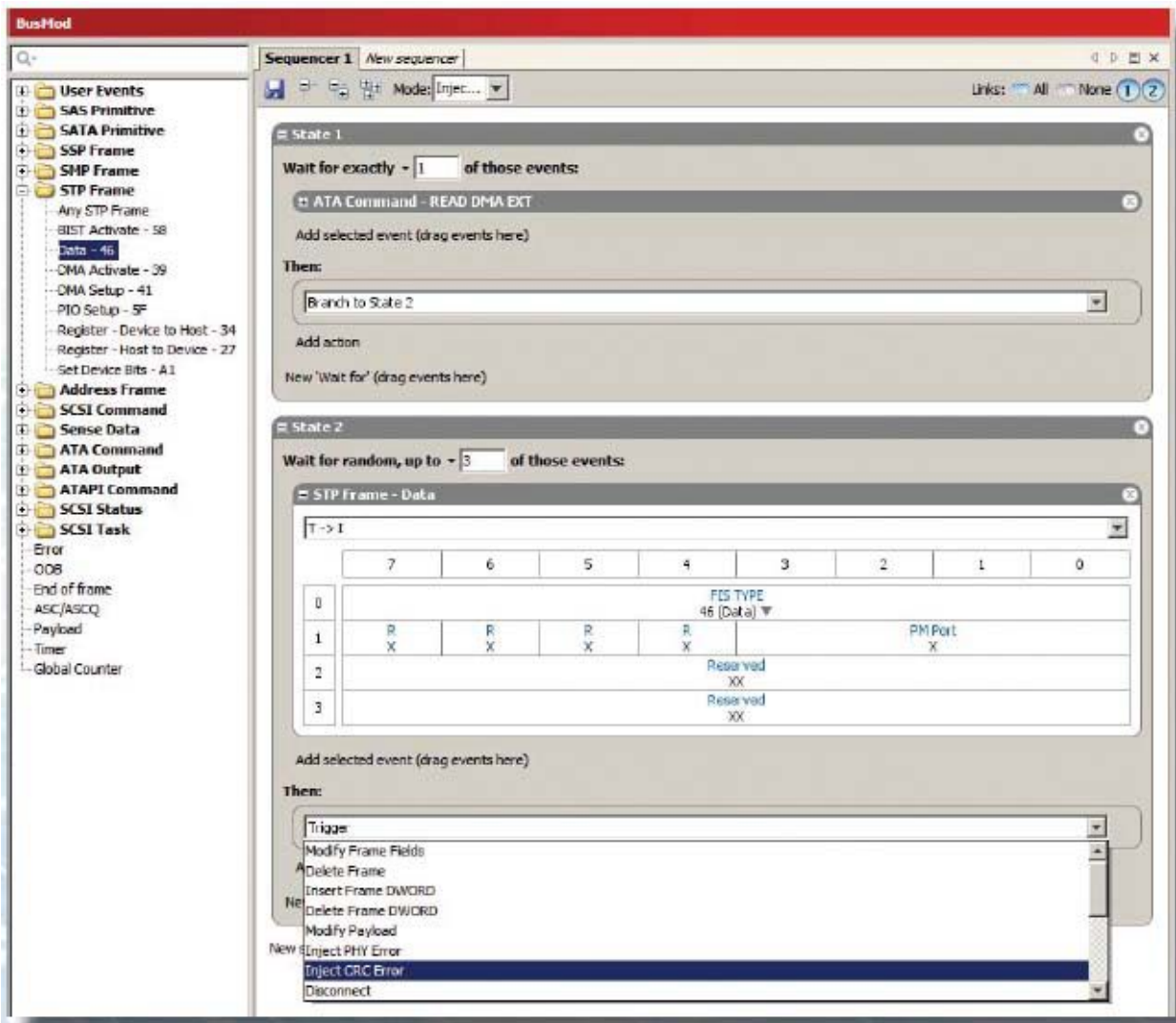


图7-16 SATA Jammer管理软件界面

通过在SATA链路上创建各种不同的错误，可以确认各种错误处理的流程是否正确或者完善，甚至增加新的流程。

Jammer还有别的用处，当你想知道某种场景（Scenario）发生以后主机或者设备的反应时，可以通过Jammer来知道答案。比如当设备回复的SDB里面Error Bit被置上，或者设备一直不发SDB时，主机是不是会重发命令，重发几次，重发多次设备都没反应的话Driver会不会启动OOB，Application会不会报错？

Jammer——你值得拥有。

7.4 回归测试

SSD这行，固件的兄弟姐妹挺不容易的：

- 有新的功能要加代码；
- 有bug要修要改代码；
- 需求变了要改代码；
- 优化性能更要改代码。

这样改来改去，改着改着就有可能把本来没问题的地方改出问题。比如，修Bug B的时候，把上个月解决的Bug A给重新放出来了，或者新创建了一个Bug C。

这种改代码出现副作用的情况，在SSD固件开发过程中几乎不可避免。

有问题就要解决，站在测试的角度，解决方法就是回归测试（Regression Test）。

Regression Test是什么：

- 确保新的代码没有影响原有功能；
- 从现有功能的测试用例中选取部分或者全部出来进行测试。

每次发布新的固件，能够把之前所有测试全部跑一次当然最好，但凡是干过测试的都知道这是不可能的，就算技术上可行，人也不够，就算人够，盘也不够，就算这些都够，时间也不够，如图7-17所示。



图7-17 平衡海量测试项目与有限测试时间

选取合适的测试用例，放在回归测试里，还是有些技巧可以参考的：

- 那些经常失败的项目，比如压力测试；
- 用户肉眼可见的功能，比如跑Benchmark；
- 核心功能的测试；
- 那些目前正在进行或者刚完成的功能；
- 数据完整性测试——R/W/C；
- 边界值测试。

科学研究证明，有效的回归测试可以节省60%的bug修复时间和40%的成本。

扁鹊见蔡桓公的故事还记得吧，有病早治，有问题早解决，大家都好。

7.5 DevSlp测试

增加了DevSlp这个功能以后，SATA IO也在原有的Partial&Slumber测试的基础上特别增加了对DevSlp的测试。

新的测试要求主要是关注DevSlp状态的进出是否正常，要实现这个必须具备两点：能让设备进入DevSlp，进去以后能够侦测到DevSlp的状态。

能否进入DevSlp的问题不用讨论，如果不能进，也不用测试了。

侦测状态，通过检查SATA Status Register（SATA状态寄存器）就能够实现，这个Register的Bit[11: 8]映射到Interface Power Management（IPM）设置。读取这个寄存器就能知道AHCI控制器（主机）要求设备进入的状态。具体定义如表7-1所示。

表7-1 SATA Status Register（SATA状态寄存器）定义

状态寄存器	2h 接口处于 Partial 省电模式
0h 设备不存在或连接未建立	6h 接口处于 Slumber 省电模式
1h 接口处于工作状态	8h 接口处于 DevSlp 省电模式

通过读写这个寄存器可以知道设备能否成功地进出DevSlp。但是具体物理层上状态切换的各种时间参数（例如MDAT、DMDT、DETO等）就没办法测量了。

专业的测试需要专业的仪器，有第三方的仪器可以做这种测试，如图7-18所示。

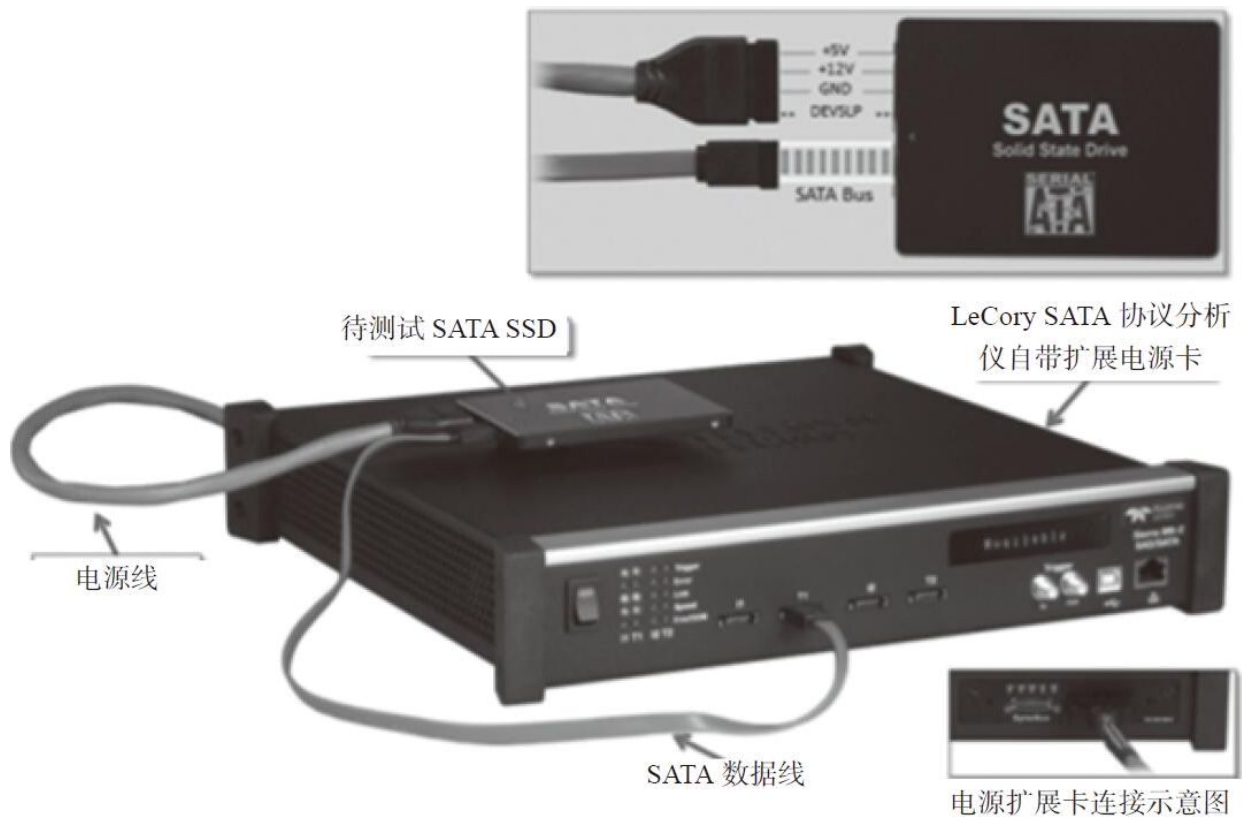


图7-18 LeCroy SATA分析仪支持DevSlp

从图中可以看到使用了专门支持DevSlp的线缆。

有两个针对DevSlp的case:

- IPM-12: Entering DevSlp Interface power state (进入DevSlp模式)。
- IPM-13: DevSlp interface power state exit latency (DevSlp模式退出时延)。

IPM-12重点是测试DevSlp进入:

- 1) 先让SSD进入DevSlp状态;
- 2) 保持DevSlp信号有效的情况下, 持续向SSD发包, 确保SSD不会回应发过去的包;

3) 检查各种时间参数是否在规定范围内（SATA 3.2里面没有包括DXET，但是测一下还是很有道理的）。

表7-2 DevSlp时序参数检查

Symbol 参数	Parameter (说明)	Value (时间要求)
MDAT	DEVSLP 最小置位时间	10ms
DMDT	DEVSLP 最小侦测时间	10μs
DXET	DEVSLP 最大进入时间	100ms
DETO	设备 DEVSLP 退出超时时间	20μs (除非在标识数据日志中另有规定)

图7-19是SATA Analyzer记录的测试结果。

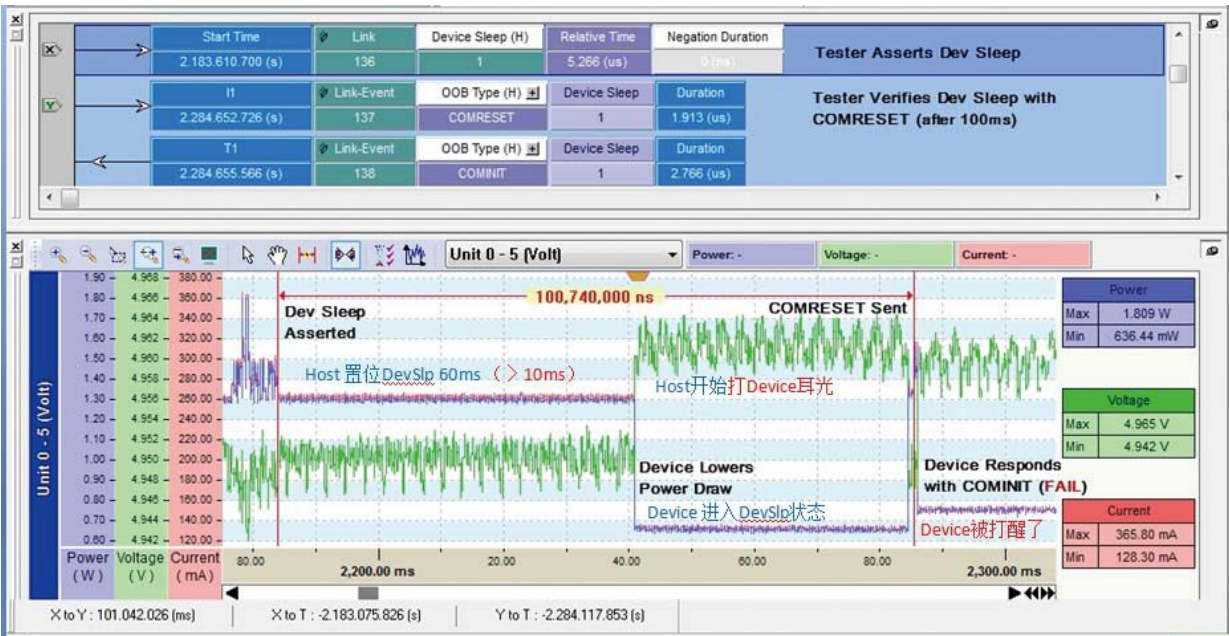


图7-19 IPM-12DevSlp测试结果

MDAT: 协议规定主机唱摇篮曲给设备听，至少要唱10ms，主机说到做到，唱了10ms又10ms，唱了10ms又10ms。

DXET: 协议规定从主机唱摇篮曲100ms以后，设备必须睡着，设备也说到做到，60ms的时候睡着了。

协议规定，设备进入DevSlp后，只要DevSlp还是置位状态，主机随便怎么弄，设备都不能醒，于是主机为了考验设备，100ms后开始不停地发COMRESET要想唤醒设备。

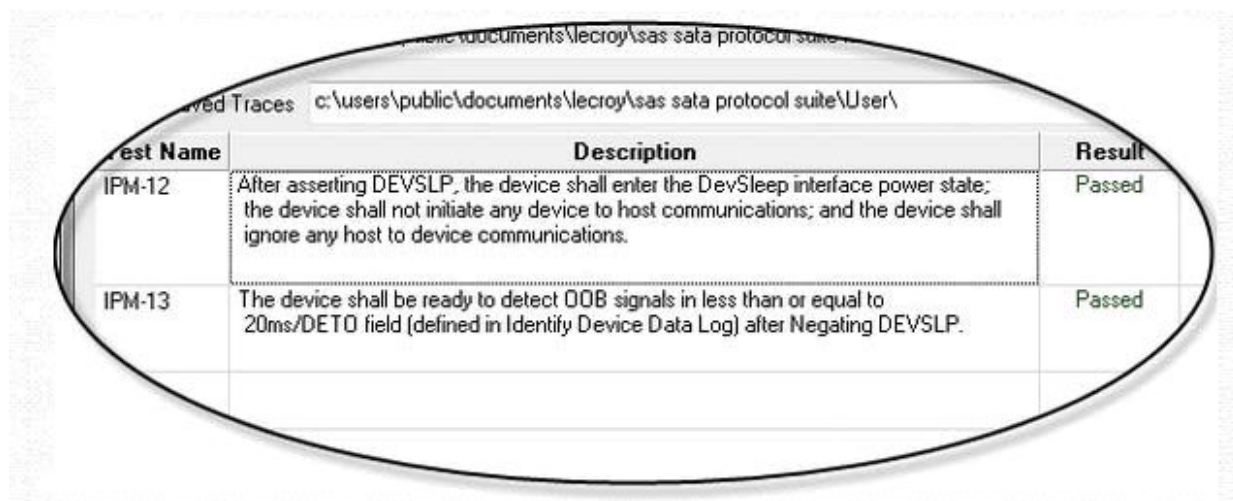
若设备能够在DevSlp的状态下能够Detect到COMRESET，说明测试失败，该功能没有做对。

IPM13的重点是测试DevSlp退出：

·退出DevSlp并不需要完整的上电流程，而是使用COMWAKE信号让SATA链路快速进入PHY Ready状态；

·DETO：协议规定设备从DevSlp状态下退出需要在20ms内完成。先Assert DevSlp信号让设备进入DevSlp状态，然后De-Assert DevSlp信号开始发送OOB信号（同时启动一个Timer），设备必须在20ms内响应OOB信号。——只要响应了就算测试通过，能不能完成OOB，IPM13不管，那是OOB测试的事情。

图7-20是最终测试结果的截图。



The screenshot shows a table with three columns: Test Name, Description, and Result. The table is titled 'Saved Traces' and the path is 'c:\users\public\documents\lecroy\sas sata protocol suite\User\'.

Test Name	Description	Result
IPM-12	After asserting DEVSLP, the device shall enter the DevSleep interface power state; the device shall not initiate any device to host communications; and the device shall ignore any host to device communications.	Passed
IPM-13	The device shall be ready to detect OOB signals in less than or equal to 20ms/DETO field (defined in Identify Device Data Log) after Negating DEVSLP.	Passed

图7-20 DevSlp最终测试结果

7.6 PCIe InterOp

PCISIG是个大家庭，没事会弄个Compliance Workshop，各公司可以把自己的产品拿去测试，包括：

·Electrical Testing: 电气化测试，重点测试物理层的发送端和接收端。

·Configuration Testing: PCIe设备配置空间测试。

·Link Protocol Testing: 设备链路层协议相关测试。

·Transaction Protocol Testing: 事务层协议测试。

·Platform BIOS Testing: 平台BIOS测试。

贵司弄出一块PCIe SSD，如果能走完这一套流程，说明PCIe接口这块没啥问题了，毕竟这些测试项目是由制定PCIe协议的组织出品的。

然后PCISIG会给贵司一个小红花，将这块PCIe SSD放到光荣榜上（Integrators List），如表7-3所示。

PCISIG光荣榜即Integrators List，网址：
<https://pcisig.com/developers/integrators-list>。

表7-3 PCIe Integrators列表示例

公司	产品	类型	速度	带宽	功能	发布日期
AMD	Device 2		PCIe 3.0 at 8GT/s	x8	Graphics	21-Jun-17
SAMSUNG Electronics	983 M.2	PCIe SSD	PCIe 3.0 at 8GT/s	x4	SSD Endpoint Card	10-Aug-17
SK hynix	PE4011	SSD Endpoint	PCIe 3.0 at 8GT/s	x4	PCIe NVMe	23-Aug-17

(续)

公司	产品	类型	速度	带宽	功能	发布日期
AMD	Device 1		PCIe 3.0 at 8GT/s	x8	Graphics	21-Jun-17
Beijing Starblaze Technology Co., LTD.	STAR1000		PCIe 3.0 at 8GT/s	x4		19-Oct-17
Beijing Memblaze Technology Co., Ltd.	PBlaze5	Memblaze NVMe SSD	PCIe 3.0 at 8GT/s	x8	NVMe SSD	23-Aug-17
Huawei Technologies Co., Ltd	SmartIO-NIC-2	PCIe Ethernet Adapter	PCIe 3.0 at 8GT/s	x16	Smart Ethernet Adapter	18-Oct-17
Realtek Semiconductor Corp.	RTS5762-CG	PCIe NVMe SSD Controller	PCIe 3.0 at 8GT/s	x4	PCIe NVMe SSD Controller	18-Aug-17

以上环节，贵司都是一个人在战斗，就像比武招亲，只能跟你未来老婆打，不能跟别的选手接触（这个比武招亲是一妻多夫制）。

Workshop里还有一个华山论剑的环节，各家公司可以把自家产品拿出来跟其他公司的产品放到一起切磋一下，看看互相之间组队有没有问题，这个环节就是Interoperability Test。

贵司拿着刚出炉的PCIe SSD，走到牙膏厂公司的展位：“兄台，小弟这有一块PCIe Gen3x4的NVMe SSD，想跟您的S主芯片切磋一下，请赐教！”牙膏厂的兄弟瞟了一眼你的Badge，亲切地拒绝了。（在这个环节，确实可以礼貌地拒绝。）

按摩店A公司在忙着跟S公司、M公司玩，也暂时没空搭理贵司。

这时，和蔼可亲的Synopsys凑了上来：“这位小兄弟，我看你骨骼清奇，未来必成大器……”于是你们两家摆开阵势，按照下面流程开始切磋：

1) 了解对方的实力（就像相亲时问对方：你们小区停车费多少钱一个月？），通过Link Capability Register（链路能力寄存器）了解双方各自的链路速度[3: 0]和带宽[9: 4]，如图7-21所示。

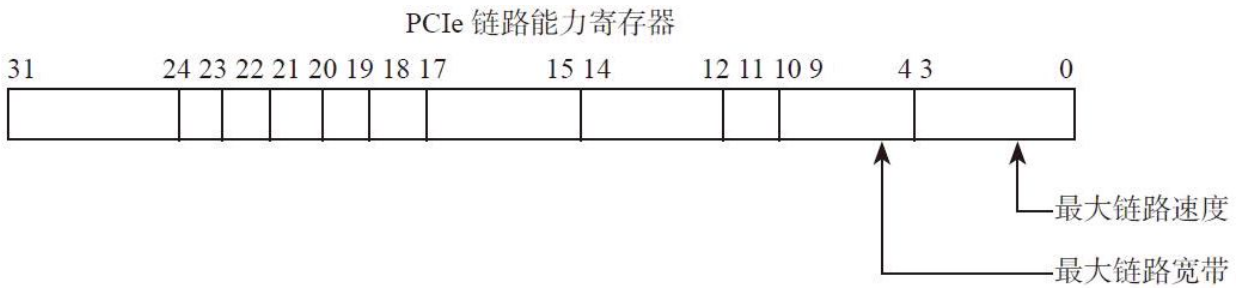


图7-21 PCIe链路能力寄存器

- 2) 假设贵司PCIe SSD最高到Gen3x4（链路速度Gen3，带宽为x4），Synopsys RC最高到Gen3x16。
- 3) 把你的PCIe SSD插到Synopsys带来的开发板上（Synopsys卖IP，不卖产品）。
- 4) 开机，检查你的PCIe SSD被OS识别到（过程中可能会提示安装驱动），检查Link Status Register确定link状态是Gen3x4，如图7-22所示。

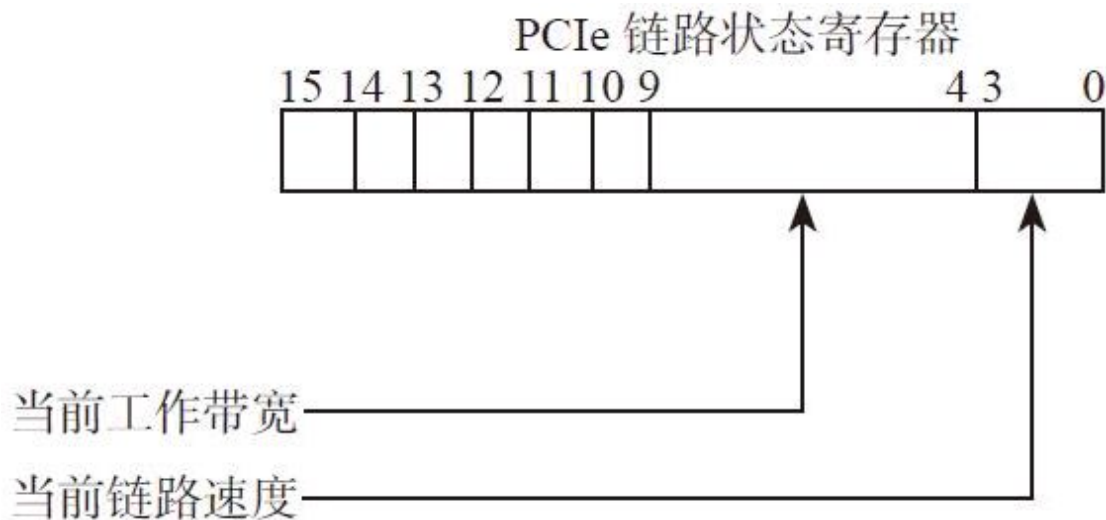


图7-22 PCIe Link Status Register

- 5) 如果你的PCIe SSD还支持其他lane width——比如x1，用胶布或者Reducer把lane width降到x1，重复上述步骤，确保x1也能正常工作。
- 6) Speed和Width正确还不够，还需要做一下简单的数据传输，确保数据能顺利通过PCIe Bus。

PCISIG贴心地为初入江湖的你提供了方便查看PCIe Register的工具——PCITree: <http://www.pcitree.de/>。

以上都顺利通过，把你们俩的交手记录上传到PCISIG的服务器上，继续去找其他RC或者Switch供应商。

写在最后，台上一分钟，台下十年功，为了在Workshop的Interoperability环节有好的表现，在下山前就应该找来各家的RC做相关的测试。

比如先定一个能达到的小目标，Intel、ASUS、Gigabyte最新、次新的主板来个10块，开机上电检查Link Speed/width，每台机器先过个200次（此处需要Automation）。

7.7 WA测试

WA的计算公式： $WA = \text{闪存写入的数据量} / \text{主机写入的数据量}$ 。

只要知道了A（闪存写入的数据量）和B（主机写入的数据量）就可以知道WA了。

这两个数据，从哪里拿？从SMART信息里。

《【原创】浴室谈SSD的SMART信息》里面列举了几款SSD产品的SMART信息，如表7-4所示是SandForce 12xx/15xx主控的信息。

原文链接：<http://bbs.pceva.com.cn/thread-10212-1-1.html>。

表7-4 SandForce 12xx/15xx主控SMART信息

编号	含义	属性
1	Raw Read Error Rate	底层数据读取出错率
5	Retired Block Count	不可使用的坏块计数

(续)

编号	含义	属性
9	Power On Hours Count	累计加电时间
12	Power Cycle Count	设备通电周期
171	Program Fail Count	编程错误计数
172	Erase Fail Count	擦除错误计数
174	Unexpected Power Loss Count	不正常掉电次数
177	Wear-Range Data	显示最大磨损块和最小磨损块相差的百分比
181	同 171 定义相同	
182	同 172 定义相同	
187	Reported Uncorrectable Errors	不可修复错误计数
194	显示温度的，基本可以忽略	
195	On the Fly Reported Uncorrectable Error Count	实时不可修复错误计数
196	Reallocated Event Count	重映射坏块计数
231	SSD Life left	SSD 剩余寿命（新盘为 100，显示为 10，代表 P/E 用完了，但是还有备用空间可以替换，显示 0 则代表盘上数据为只读）
241	lifetime write from host	来自主机的写入数据量总数
242	lifetime read from host	来自主机的读取数据量总数

可以看到241: Lifetime write from host就是“主机写入的数据量”。

这张表里没有“闪存写入的数据量”，引入第二个公式：闪存写入数据量=平均Wear Leveling count×SSD容量（这个好理解吧）。

SSD容量大家都知道。Wear Leveling count，在上面这张表里没有，但是有“172Erase Fail Count（擦除错误计数）”和“177Wear-Range Data（显示最大磨损块和最小磨损块相差的百分比）”。说明FW其实统计了Wear Leveling count，只是没有显示出来。

这篇文章里提到了另外一款SSD——美光C300，其包括Marvell 88SS9174主控和美光自己的固件，就直接公布了参数：“173Wear Leveling Count（平均擦写次数）”，但没有公布“241Lifetime write from host”。

上述这些在内部测试的时候都不是问题，请FW的兄弟们把这两项都显示出来，测试工程师可以计算自家SSD的WA了。

7.8 耐久度测试

一款SSD出货前必须要经过严格的耐久度（Endurance）测试，简单说来就是SSD有多经用。JEDEC有两份SSD Endurance测试的协议，分别是：

- JESD 218A：测试方法。

- JESD 219： workload。

首先需要了解如下概念：

- TBW： 总写入数据量。

- FFR（Function Failure Requirement）： 整个写入过程中产生的累计功能性错误。

- Data Retention： 长时间不使用（上电）情况下保持数据的能力。

- UBER（Uncorrectable Bit Error Rate）： $UBER = \text{number of data errors} / \text{number of bits read}$ 。

企业级和消费级SSD在耐久度的要求上是不同的，体现在：

- 工作时间；

- 工作温度；

- UBER；

- Retention温度以及时间。

具体数据如表7-5所示。

表7-5 消费级与企业级SSD可靠性测试要求

产品类别	工作负载 (参考 JESD219)	工作条件 (上电状态)	数据保存 (断电状态)	FFR (Functional Failure Requirement) 功能性失效要求	UBER Requirement 不可恢复误码率
消费级	消费级	40℃ 8 小时 / 天	30℃ 1 年	$\leq 3\%$	$\leq 10^{-15}$
企业级	企业级	55℃ 24 小时 / 天	40℃ 3 个月	$\leq 3\%$	$\leq 10^{-16}$

虽然叫耐久度测试，但是218其实是包括了耐久度和数据保持（Data Retention）两部分测试的，官方给的方法有两种：

- Direct method——直来直去法。
- Extrapolation method——拐弯抹角法。

本书着重解释Direct method，理解了它以后，另一个方法就很容易理解了。

Direct method，简单来说，就是使劲写，可劲读，套用贝爷的口头禅：“Push the SSD to limit”，在这个过程中，要注意：

- 要求有高低温；
- 必须用指定的workload；
- 耐久度测试以后马上进行数据保持测试。

在详细介绍这些之前，首先要搞明白一个问题，应该拿多少块SSD跑耐久度测试？

要求一：如果该系列SSD首次进行测试，选取的SSD要来自至少三个不连续的生产批次，如果不是首次，选一个批次的就行。

要求二：制定标准时直接给了两个公式。

·UCL (functional_failures) \leq FFR \times SS (for Functional Failure)

·UCL (data_errors) \leq min (TBW, TBR) $\times 8 \times 10^{12} \times$ UBER \times SS (for Data Failure)

如果只看公式，你可能会跟我一样，一脸懵。其中：

- Functional failure：可以接受的出现功能故障的SSD的数量；

- Data_error: 可以接受的数据出错的数量;
- TBW, TBR: 总写入/读取量;
- SS: Sample Size, 就是我们要求的X (用多少块盘测试);
- UCL: Upper confidence Limit函数, 看不懂是不是, 不用你看懂, 直接查表就行 (见表7-6)。

表7-6 UCL函数查值表

AL	n	AL	n	AL	n	AL	n	AL	n
0	0.92	20	21.84	40	42.30	60	62.66	80	82.97
1	2.03	21	22.87	41	43.32	61	63.68	81	83.98
2	3.11	22	23.89	42	44.35	62	64.69	82	84.99
3	4.18	23	24.92	43	45.36	63	65.71	83	86.00
4	5.24	24	25.94	44	46.38	64	66.72	84	87.02
5	6.29	25	26.97	45	47.40	65	67.74	85	88.03
6	7.34	26	28.00	46	48.42	66	68.75	86	89.05
7	8.39	27	29.02	47	49.43	67	69.77	87	90.06
8	9.43	28	30.04	48	50.46	68	70.79	88	91.08
9	10.48	29	31.07	49	51.47	69	71.80	89	92.08
10	11.52	30	32.09	50	52.49	70	72.82	90	93.10
11	12.55	31	33.12	51	53.51	71	73.83	91	94.11
12	13.59	32	34.14	52	54.52	72	74.85	92	95.13
13	14.62	33	35.16	53	55.55	73	75.86	93	96.14
14	15.66	34	36.18	54	56.56	74	76.88	94	97.15
15	16.69	35	37.20	55	57.58	75	77.89	95	98.16
16	17.72	36	38.22	56	58.60	76	78.91	96	99.18
17	18.75	37	39.24	57	59.61	77	79.92	97	100.19
18	19.78	38	40.26	58	60.63	78	80.94	98	101.21
19	20.81	39	41.29	59	60.64	79	81.95	99	102.22

通常我们直接用AL=0 (AL=0代表没有functional failure), 这样对应的UCL就是0.92。

这里结合一个实际的例子说明, 假设FFR=3%, UBER= 10^{-16} , TBW=100, 代入公式得到:

$$\cdot SS \geq 0.92 / (0.03) = 30.1$$

$$\cdot SS \geq 0.92 / (100 \times 1 \times 8 \times 10^{12} \times 10^{-16}) = 11.5$$

两个SS分别能够满足Functional Failure和Data Failure的要求，取两者之间的较大值30.1，所以需要的跑测试的SSD数量是31块。

再把SS=31代入公式：UCL (data_errors) $\leq 100 \times 1 \times 8 \times 10^{12} \times 10^{-16} \times 31 = 2.48$

用2.48这个值去表（见表7-7）里反查，得到允许的最大data errors数量为1。

表7-7 表格反查获得最大Data Error值

AL	n	AL	n	AL	n	AL	n	AL	n
0	0.92	20	21.84	40	42.30	60	62.66	80	82.97
1	2.03	21	22.87	41	43.32	61	63.68	81	83.98
2	3.11	22	23.89	42	44.35	62	64.69	82	84.99
3	4.18	23	24.92	43	45.36	63	65.71	83	86.00
4	5.24	24	25.94	44	46.38	64	66.72	84	87.02
5	6.29	25	26.97	45	47.40	65	67.74	85	88.03
6	7.34	26	28.00	46	48.42	66	68.75	86	89.05
7	8.39	27	29.02	47	49.43	67	69.77	87	90.06
8	9.43	28	30.04	48	50.46	68	70.79	88	91.08
9	10.48	29	31.07	49	51.47	69	71.80	89	92.08
10	11.52	30	32.09	50	52.49	70	72.82	90	93.10
11	12.55	31	33.12	51	53.51	71	73.83	91	94.11
12	13.59	32	34.14	52	54.52	72	74.85	92	95.13
13	14.62	33	35.16	53	55.55	73	75.86	93	96.14
14	15.66	34	36.18	54	56.56	74	76.88	94	97.15
15	16.69	35	37.20	55	57.58	75	77.89	95	98.16
16	17.72	36	38.22	56	58.60	76	78.91	96	99.18
17	18.75	37	39.24	57	59.61	77	79.92	97	100.19
18	19.78	38	40.26	58	60.63	78	80.94	98	101.21
19	20.81	39	41.29	59	61.64	79	81.95	99	102.22

总结：选31块盘，跑完耐久度测试，不能有Functional failure，最多可以有1个Data-error，测试才会通过。

耐久度测试使用的workload可以从网上下载，整个workload大概有4亿条Write、trim、flush命令（消费级SSD），每次写完之后需要read回来确保数据是正确的，具体实现的工具没有要求。

耐久度和数据保持过程中另一个重要的因素就是高低温。

具体的温度要求如表7-8所示，可以看到企业级SSD要求比消费级SSD高出不少。

表7-8 消费级与企业级SSD可靠性测试温度要求

产品类别	工作条件 (上电状态)	数据保存 (断电状态)	耐久度测试温度要求 (Endurance Stress Temperature)	数据保持测试温度要求 (High Temperature Retention Stress Temperature)
消费级 (Client)	40℃ 8 小时 / 天	30℃ 1 年	Ramped Approach: 低温: $T \leq 25^{\circ}\text{C}$ 高温: $40^{\circ}\text{C} \leq T \leq T_{\max}$ Split-flow Approach: 低温: $T \leq 25^{\circ}\text{C}$ 高温: $40^{\circ}\text{C} \leq T \leq T_{\max}$	96 小时 / $T \geq 66^{\circ}\text{C}$ 或者 500 小时 / $T \geq 52^{\circ}\text{C}$
(续)				
产品类别	工作条件 (上电状态)	数据保存 (断电状态)	耐久度测试温度要求 (Endurance Stress Temperature)	数据保持测试温度要求 (High Temperature Retention Stress Temperature)
企业级 (Enterprise)	55℃ 24 小时 / 天	40℃ 3 个月	Ramped Approach: 低温: $T \leq 25^{\circ}\text{C}$ 高温: $60^{\circ}\text{C} \leq T \leq T_{\max}$ Split-flow Approach: 低温: $T \leq 25^{\circ}\text{C}$ 高温: $60^{\circ}\text{C} \leq T \leq T_{\max}$	96 小时 / $T \geq 66^{\circ}\text{C}$ 或者 500 小时 / $T \geq 52^{\circ}\text{C}$

控制温度变化有两种策略：

·Ramped-Temperature approach: 所有SSD放在一起，在高低温间来回切换。

·Split Flow approach: 所有SSD分两半，一半进行低温测试，一半进行高温测试。

低温没有问题，要求 $\leq 25^{\circ}\text{C}$ 。

高温的要求是一个区间，比如Client SSD的高温温度区间是 $40^{\circ}\text{C} \leq T \leq T_{\max}$ ，高温下限是 40°C ，上限没有给出具体数值。

在JESD-218A的附录里介绍了通过温度对Endurance和Retention测试的时间加速作用，有兴趣的读者可以自行参阅。其论证的结论就是温度越高，就能用越短的时间模拟出对SSD进行1年读写的效果，对应关系如表7-9所示。

表7-9 温度加速时间对照表

实际压力测试时间（小时）	Split 策略		Ramped 策略	
	消费级	企业级	消费级	企业级
50	79	105	86	113
100	72	98	79	105
150	68	93	75	101
200	66	90	72	98
250	64	88	70	95
300	62	86	68	93
350	61	85	67	92
400	60	83	66	90
450	59	82	65	89
500	58	81	64	88
...				
2500	44	66	50	72
3000	43	64	48	71

以第一行为例，采用Ramped temperature方式，当高温达到86℃时，对一块盘进行50小时的读写（必须用官方的workload）能够达到常温下一年的效果。

而同样的SSD，如果高温只有48℃（最后一行），必须跑3000小时的读写才能达到一样的效果。

那怎样确定这个 T_{max} 呢？我理解的步骤是这个样子：

·根据SSD容量计算器TBW，比如160GB的TLC SSD，按PE cycle 500计算其TBW应该是80TB。

·workload来一遍为1TBW。

·那么总共需要把workload跑上80遍。

·假设跑一遍workload需要5个小时。

·那么总时间就是400小时。

·在表7-9中找到与400小时对应的温度为66°C (Client SSD, Ramped)，这个就是 T_{\max} 值。

有了workload，知道了温度范围，就可以正式跑Endurance测试了，图7-23是Direct Method使用Ramped approach的流程图。



图7-23 SSD耐久度测试Direct Method Ramped Approach流程图 [\[1\]](#)

从上到下整个过程分别是：

- 1) Sample取样，确定用多少块SSD测试；
- 2) 耐久度测试；
- 3) 部件级常温数据保持测试（可选）；
- 4) 写入数据，为了后面的数据保持测试；
- 5) 产品级常温数据保持测试（可选）；
- 6) 高温数据保持；
- 7) 数据比较；
- 8) 判断是否通过（检查FFR和Data_error是否满足前面那两个公式）。

步骤1、2已经介绍过，步骤3~7都是关于Data retention的，这个测试要求在耐久度测试结束以后马上进行：写入数据→断电→高温→上电→数据比较。

而对于某个系列的首次耐久度测试，还要求进行常温数据保持测试，详细情况可以参考JESD218A 7.1.5测试标准。

最后简单提几句Extrapolation method，说白了就是用各种方法在最短的时间完成Endurance测试，比如：

修改workload，在更短的时间内造成更多的PE cycle（修改随机/顺序访问占比，传输数据大小，引发更多background activity等）。

限制SSD的大小，比如把前面的160G SSD通过固件限制为40G可用，那么所需要的Endurance时间就直接从400小时降低到100小时（相应高温需要从66℃调整为79℃），如图7-24所示。

实际压力测试 时间（小时）	Split 策略		Ramped 策略	
	消费级	企业级	消费级	企业级
50	79	105	86	113
100	72	98	79	105
150	68	93	75	101
200	66	90	72	98
250	64	88	70	95
300	62	86	68	93
350	61	85	67	92
400	60	83	66	90
450	59	82	65	89
500	58	81	64	88

图7-24 通过提高温度减少可靠性测试的时间

特别要注意的是，固件在限制大小的时候，不仅要限制开放给主机的读写区域，同时内部的OP空间也必须同样等比例缩小。

[1] 图中的章节为该测试规范中的章节。

7.9 认证Certification

一款SSD研发出来，除了内部的层层测试，也少不了送出去进行各种认证测试。

1.SATA-IO Plugfest和IW（Interoperability Workshop）

作为SATA协议的官方组织，SATA-IO每年都会组织厂商一起坐坐，给大家一个互相切磋的机会进行兼容性、交互性以及新功能的测试。

图7-25所示是2008年的活动日程表，Plugfest三天，IW五天。

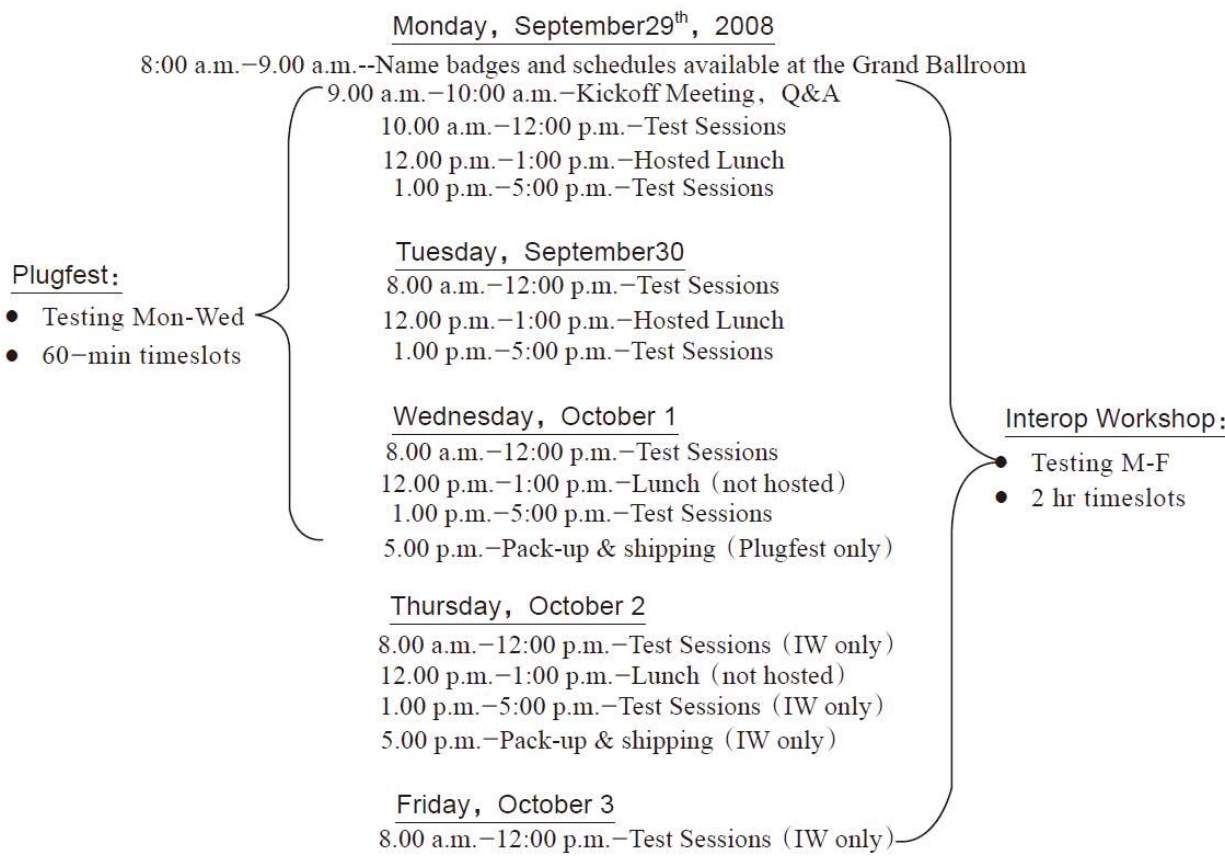


图7-25 SATA-IO Event日程示例

2.IW和Plugfest有所不同

IW的对象是量产产品，由SATA-IO主导，有固定的测试流程和项目，并且测试结果需要提交SATA-IO，通过测试的设备可以加入Integrators List。

Plugfest的对象是开发阶段的产品，厂商之间互相玩耍，测什么，怎么测，大家自己说了算，测试结果不用提交给SATA-IO。

官方网站上有具体介绍以及报名方式：

<https://www.sata-io.org/plugfests>

<https://www.sata-io.org/interoperability-workshops>

3.PCIe SIG Compliance Program

作为PCIe协议的官方组织，PCIe SIG的一致性测试项目包括以下方面：

- Electrical Testing: 针对平台和卡的Tx和Rx电器性能进行测试。
- Configuration Testing: PCIe configuration space测试（Tool: PCIE CV）。
- Link Protocol Testing: 针对设备进行链路层协议测试。
- Transaction Protocol Testing: 针对设备进行传输层协议测试。
- Platform BIOS Testing: 针对平台BIOS进行测试，判断其能否识别并正确配置设备。

通过PCIe SIG的测试同样可以加入Integrators List。

官方网站上提供Test Guide下载，包括测试描述、规格、流程以及相关的工具：

<https://pcisig.com/developers/compliance-program>

4.UNH IOL NVMe Test

UNH-IOL全称是University of New Hampshire InterOperability Laboratory，是业界著名的公开实验室，提供多个领域的测试服务。图7-26所示为这个实验室涉及的领域。



图7-26 IOL交互性测试实验室涉及领域

UNH-IOL定义了NVMe Test Suites，包括：

- NVMe Conformance Test Suite
- NVMe Interoperability Test Suite

Test Suite会跟着NVMe Spec更新持续更新，厂商可以自行下载使用。

链接: <https://www.iol.unh.edu/testing/storage/nvme/test-suites>

UNH-IOL贴心地提供了NVMe的测试工具:

·IOL INTREACT PC EDITION Software: 基于UNH-IOL自己的NVMe Conformance Test Suite开源项目的工具，图形界面上手容易。

·IOL INTERACT Teledyne-LeCroy EDITION Software: 高级版本，必须配合LeCroy的PCIe Exerciser和Analyzer使用，能够自动跑完NVMe Conformance Test Suite里面要求的测试，而且能够自动抓取trace以供分析。

链接: <https://www.iol.unh.edu/solutions/test-tools/interact>

免费是为了更好地收费，如果使用UNH-IOL的测试服务并完成下列指定项目，就可以加入NVMe Integrators List:

- Conformance testing using IOL INTREACT PC EDITION Software;
- Conformance testing using IOL INTERACT Teledyne-LeCroy EDITION Software;
- Interoperability testing using VDbench software。

链接: <https://www.iol.unh.edu/testing/storage/nvme>。

7.10 SSD Performance测试

SNIA给Client SSD与Enterprise SSD都制定了Performance Test（性能测试）的规范，可以到其网站www.snia.org下载。

要进行SSD的Performance Test，首先要理解几个关键概念。

·**FOB: Fresh Out of Box**，指的是刚开封、全新的盘，此时SSD的性能类似于悟饭同学的愤怒形态，战斗力爆表但不持久，这并不是这块盘在未来正常使用过程中的真实能力。

·**Transition**：经过一段时间的读写，战斗力逐步降低，趋向于稳定状态，这个过程称为转换状态。

·**Steady State**：战斗力数值稳定在一个区间，Performance相关的数据，例如Throughput（吞吐量）、IOPS、Latency（延迟）都必须在Steady State下获取，据此判断其到底是超级赛亚人，还是战五渣。

看看图7-27，不同的盘Performance数据有所不同，但趋势一样：爆表→下降→稳定。

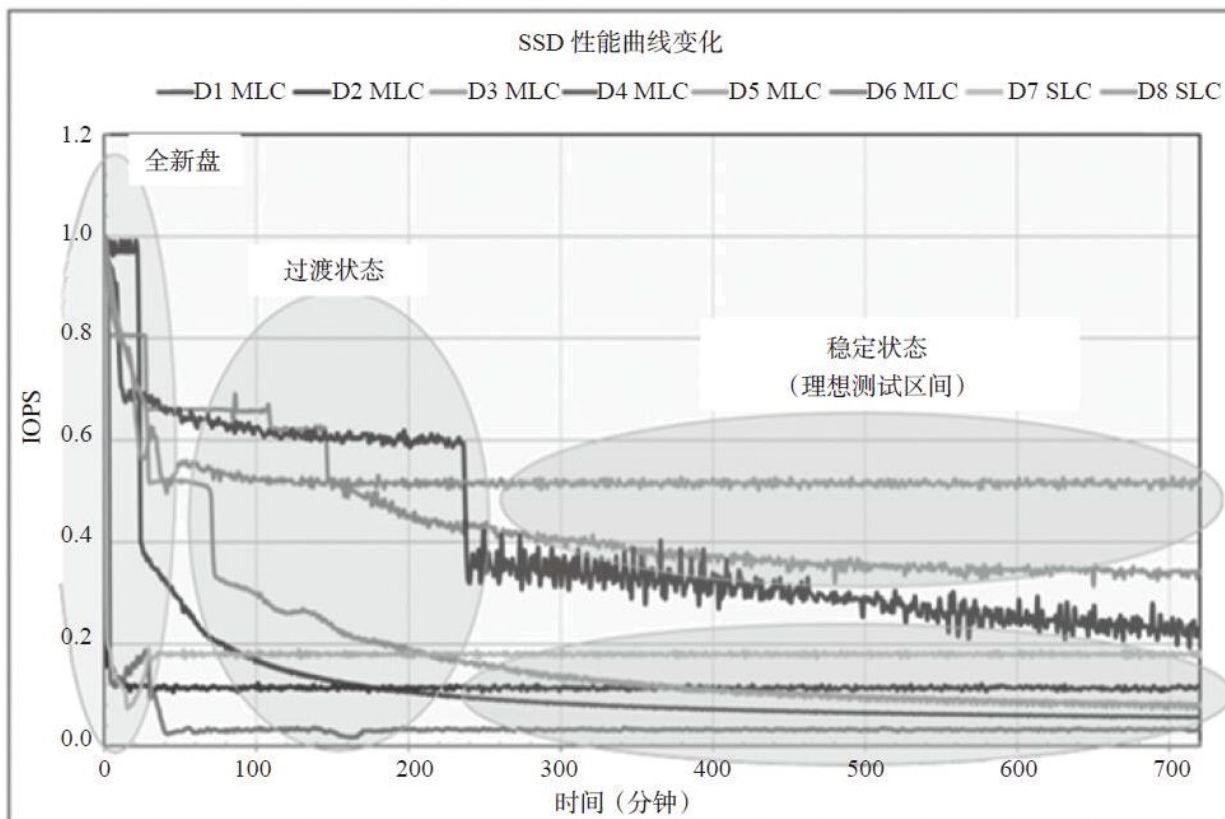


图7-27 SSD性能变化趋势

Steady State（稳定态）的判断原则是：这段时间内性能波动不超过 $\pm 10\%$ 。

接下来，介绍另外几个概念：

1) **Purge**（擦除）：每次进行Performance测试前都必须进行Purge动作，目的是消除测试前的其他操作（读写及其他测试）带来的影响（比如，一段小BS的随机读写之后立即进行大BS的顺序读写，这时候大BS的数据会比较差），从而保证每次测试时盘都是从一个已知的、相同的状态下开始。简单来说，可以把Purge理解为：让盘回到FOB状态。

实现的Purge方法可以是：

- ATA: Security Erase, SANTIZIE Device (Block Erase Ext)。
- SCSI: FORMAT UNIT。

·Vendor specific method（厂商的工具）。

2) Precondition: 通过对盘进行IO使其逐步进入Steady State的过程，分两步进行。

·Workload Independent Preconditioning（WIPC）：第一步，读写时不使用测试的Workload。

·Workload Dependent Preconditioning（WDPC）：第二步，读写时使用测试的Workload。

3) Active Range: 测试过程中对盘上LBA发送IO命令的范围，如图7-28所示。

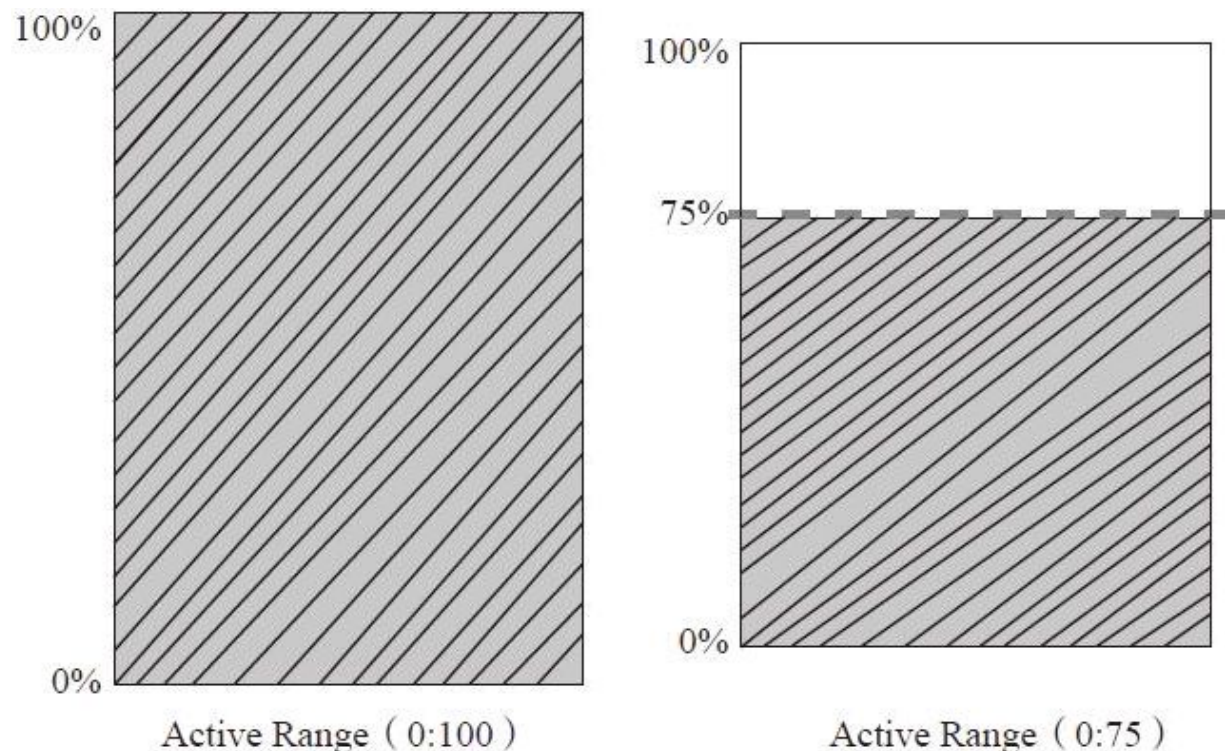


图7-28 SSD性能测试有效测试范围

4) Data pattern: Performance测试必须使用随机数据（向闪存中写入的数据）。

基本测试流程：

1) Purge the device: 擦除SSD。

2) Run Workload Independent Precondition: 比如用128K的BS顺序把盘写两遍。

3) Run Test (包括Workload Dependent Precondition): 设置好相关参数 (OIO/Thread、Thread count、Data Pattern等) 后开始进行 Workload Dependent Precondition, 最多跑25个round。

4) 假设在25个round以内达到了Steady Status, 例如第x次。那么:

- Round 1: x称为Steady Status收敛区间;

- Round (x-4): 4称为测量区间 (Measure Window)。

5) 如果25个round还没有达到Steady Status, 可以选择:

- 继续步骤3直到达到Steady Status并记录x;

- 直接取x=25。

注意: 步骤2到步骤3之间不可以中断、停顿。

Performance测试项目包括IOPS测试、Throughput测试、Latency测试和饱和写测试 (可选)。

以IOPS测试为例说明:

1) Purge SSD。

2) Workload Independent Preconditioning: 用128K的BS把SSD写两遍。

3) Workload Dependent Preconditioning and Test。

- 用RW Mix (100/0、95/5、65/35、50/50、35/65、5/95、0/100)、BS (1024KB、128KB、64KB、32KB、16KB、8KB、4KB、512B) 组合进行Random IO。

- 每个Round包括7×8=56个组合, 每个组合跑一分钟并记录结果。

·以R/W Mix=0/100，BS=4KB这个组合的IOPS结果判断是否到达Steady State（参考前文Steady State判断标准）。

·在测量区间（Measure Window）记录相关数据。

Throughput测试和Latency测试的步骤大致相同，需要注意的是：

·Throughput测试：只有两个组合——BS=1024K Sequential Write和BS=1024K Sequential Read，用Sequential Write的值来判断Steady Status。

·Latency测试：只使用3种RW Mix组合（100/0、65/35、0/100）和3种BS（8K、4K、512B），另外需要把队列数和线程数都设为1。

饱和写测试（Write Saturation Test，WST），对SSD进行长时间的Random 4K写操作，评测其经过长期写入以后的表现。

关于饱和写测试，国外知名网站TechReport.com的弟兄们曾经花了18个月，拿了6块不同厂商的SSD进行了“惨无人道”的、超过2PB的连续写入操作。

原文链接：<http://techreport.com/review/24841/introducing-the-ssd-endurance-experiment>。

中文链接：<http://www.ssfans.com/?p=672>。

Performance测试项目配置总结如表7-10所示。

表7-10 SSD性能测试配置

测试项目	读写比例	数据块大小	随机 / 顺序	Benchmark
IOPS	100/0 ~ 0/100	512B ~ 1MB	随机	Write BS=4KB
吞吐量	100/0、0/100	1MB	顺序	Write BS=1MB
时延	100/0、65/5、0/100	512B、4KB、8KB		
写饱和	0/100	4K	随机	N/A

第8章 SSD电源管理

与传统硬盘相比，SSD不仅具备更高的读写速度，能耗上也有非常大的优势。本章从SATA链路、PCIe链路、NVMe协议以及SSD内部主控管理等方面介绍SSD上的电源管理技术。

8.1 SATA省电模式Partial和Slumber

SATA链路电源管理，可以让SATA链路的PHY进入低功耗模式，与硬盘或者SSD其他部分（CPU、DDR、后端）的电源管理是完全独立的。以硬盘为例，SATA链路的电源状态与盘片的转数快慢是相互独立的。

SATA提供了两种低功耗模式：Partial和Slumber。

·Partial模式：PHY处于低功耗状态，退出时间要求 $< 10\mu\text{s}$ 。Partial是让部分物理层（PHY）电路进入休眠模式，能够在 $10\mu\text{s}$ 内被唤醒，让链路在不太影响传输性能的情况下忙里偷闲，休息一下。

·Slumber模式：PHY处于更低功耗状态，退出时间要求 $< 10\text{ms}$ 。与Partial模式相比，Slumber关闭更多的电路，因此它的恢复要慢一些，恢复时间大约为 10ms 。当预测有一段相对长的Idle时间时，会让链路好好休息一下。

在图8-1中可以看到Partial/Slumber把功耗从Active State的 1000mW 降低到了 100mW 左右。

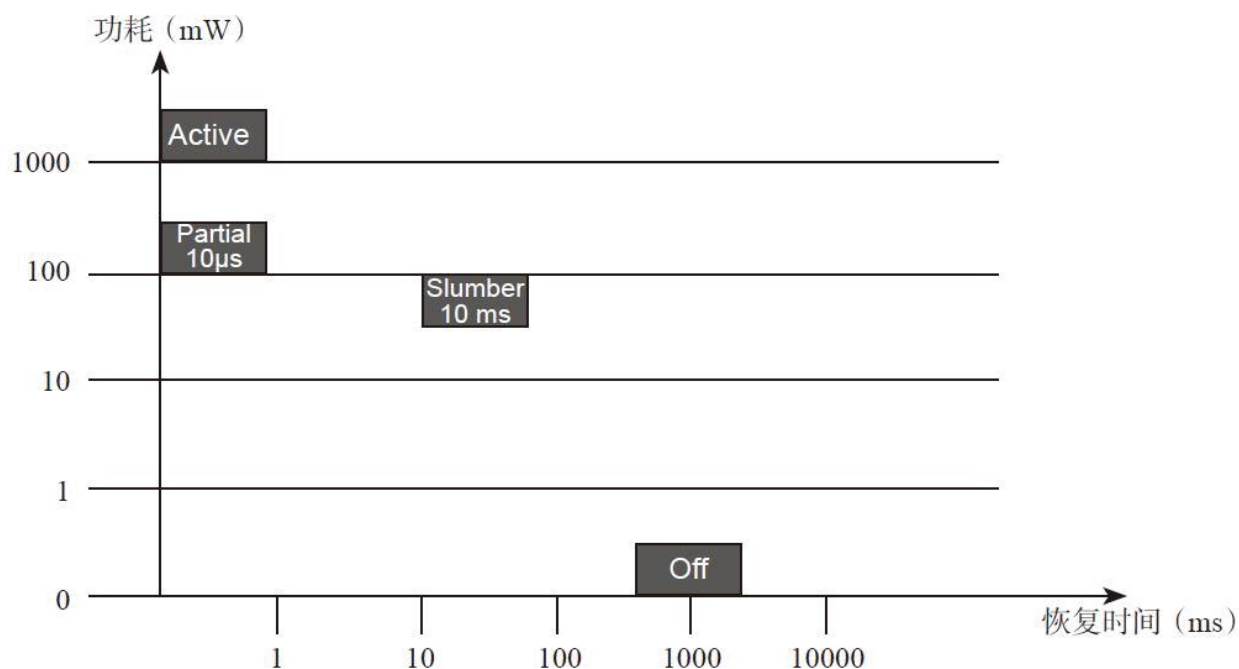


图8-1 Partial和Slumber两种模式的功耗和时延

在链路电源管理方面，SATA一视同仁，主机和设备都可以发起，分别称为：

- HIPM（Host Initiated Power Management）。

- DIPM（Device Initiated Power Management）。

发起归发起，还是需要对方配合，才能让链路进入Partial或者Slumber模式。具体做法是这样的，以主机发起为例：

- 主机发送一个PMREQ_P（请求进入Partial）给设备（如果发PMREQ_S就是请求进Slumber）；

- 设备回复PMACK（同意）或者PMNAK（不同意）；

- 如果设备回复同意，两边一起进Partial（一般接收方都会发送多个PMACK以确保发起方收到）；

- 如果回复不同意，那就什么都不发生；

- 如果需要退出Partial或者Slumber，需要通过OOB重新建立连接。

其他知识点：

- Listen Mode（侦听模式）：AHCI支持让没有接盘的端口进入侦听模式，此时该端口的功耗水平相当于Slumber，但是该端口可以识别新接入的盘。

- Auto Partial to Slumber：可以让链路不需要回到Active状态，直接从Partial进入Slumber模式。

8.2 SATA超级省电模式DevSlp

从SATA 3.2开始，SATA有了一个新的功能DevSlp（Device Sleep，设备睡眠）。DevSlp是一个信号，通过发送这个信号让盘进入一个非常省电的状态。

前文介绍过SATA允许盘进入省电模式，即Partial和Slumber模式。

Partial/Slumber省电模式下，盘都必须让自己的传输电路保持在工作模式，以便在SATA主机需要的时候能把盘唤醒。如图8-2所示，进入Partial或Slumber后，SATA总线的发送模块和接收模块仍然处于工作状态，因为这个原因，盘睡得并不安稳，省电效果也不好。

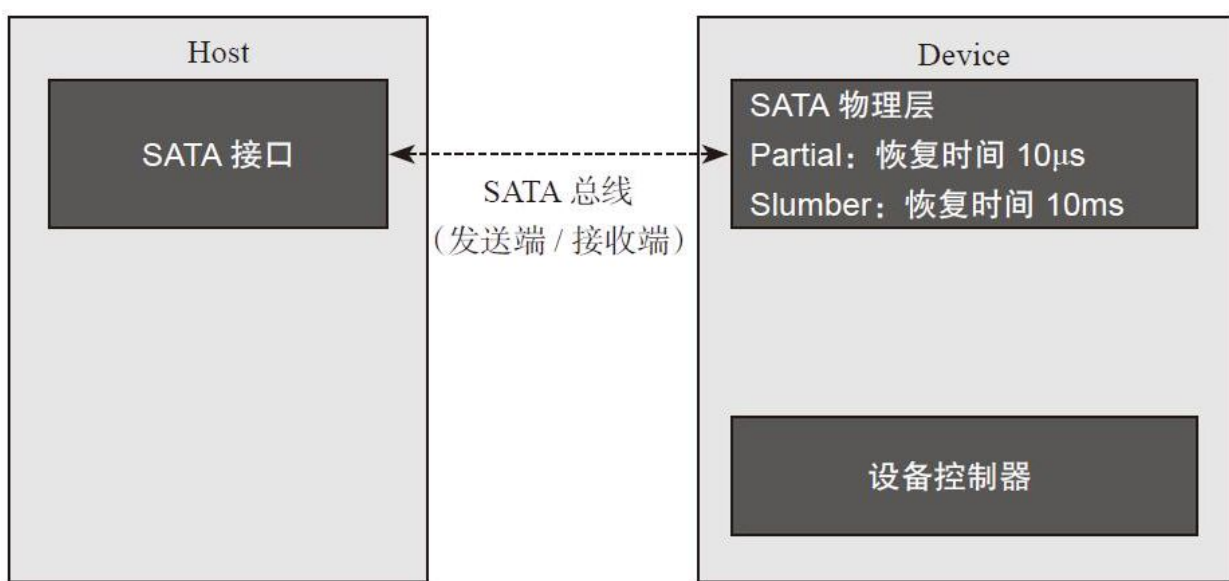


图8-2 主机与设备链接示意图

DevSlp就是把这个传输电路完全关掉，然后专门加了一个低速的管脚来负责接收唤醒通知，如图8-3所示。

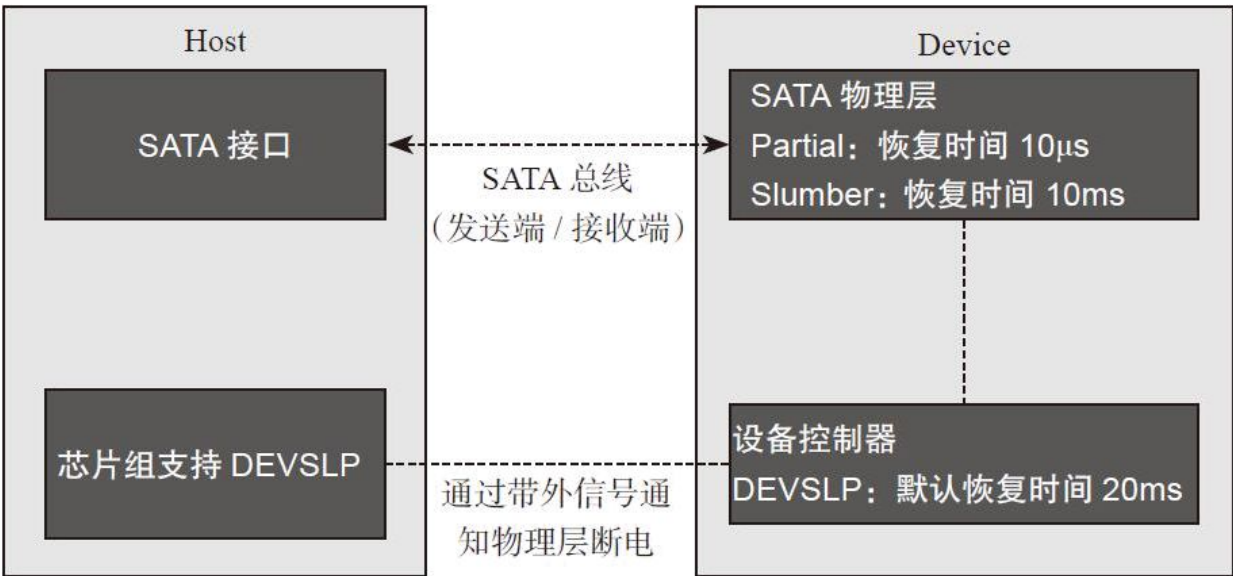


图8-3 DEVSLP的带外信号

DevSlp模式效果如图8-4所示，功耗降低到了5mW左右，而恢复时间进一步延长至20ms，但其实PC用户根本感觉不出10μs、10ms、20ms的区别。

那么问题来了，这个多出来的管脚从哪里来？

原本标准的2.5/3.5寸SATA接口上已经有多余的管脚了，SATA 3.2把管脚3单独拿出来用于DevSlp，而原本管脚1、管脚2和管脚3是用于3.3V管脚供电的。

表8-1列出了SATA 3.0的管脚定义。

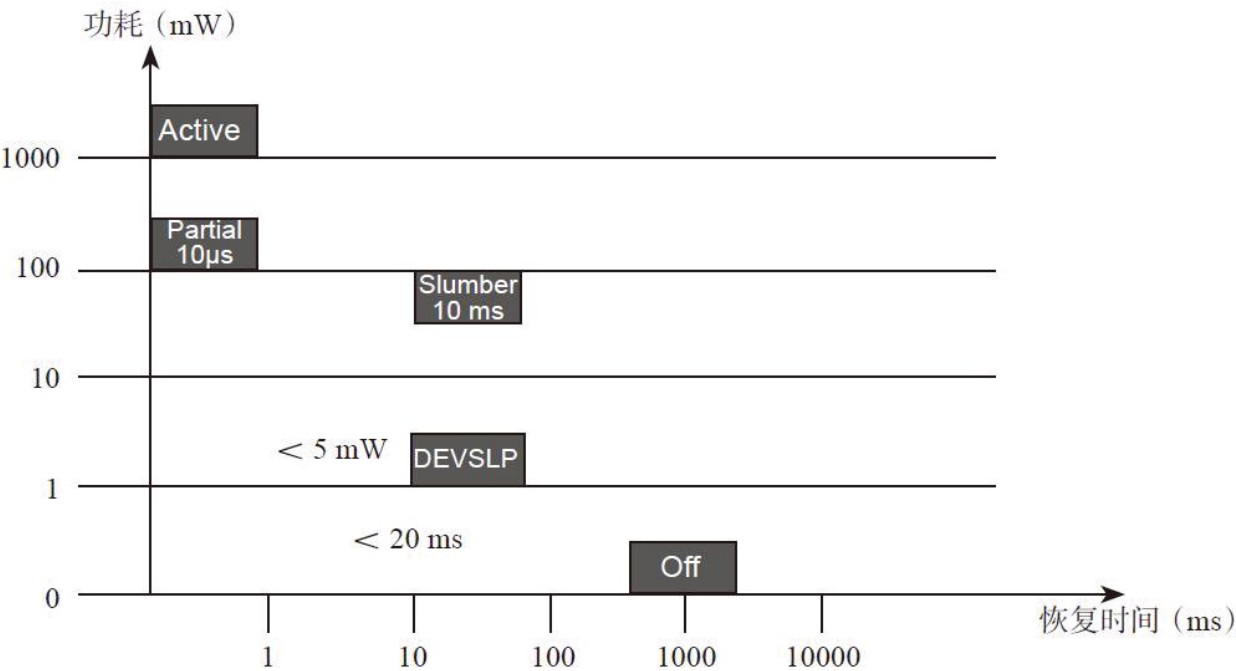


图8-4 DevSlp模式功耗时延与Partial/Slumber对比
表8-1 SATA 3.0管脚定义

	名称	类型	描述	线缆形式	背板形式
信号部分	S1	GND	差分信号组 A	1 st Mate	2 nd Mate
	S2	A+		2 nd Mate	3 rd Mate
	S3	A-		2 nd Mate	3 rd Mate
	S4	GND	差分信号组 B	1 st Mate	2 nd Mate
	S5	B-		2 nd Mate	3 rd Mate
	S6	B+		2 nd Mate	3 rd Mate
	S7	GND		1 st Mate	2 nd Mate
电源部分	P1	V33	3.3V Power	2 nd Mate	3 rd Mate
	P2	V33	3.3V Power	2 nd Mate	3 rd Mate
	P3	V33	3.3V Power, Pre-charge	1 st Mate	2 nd Mate
	P4	GND		1 st Mate	1 st Mate
	P5	GND		1 st Mate	2 nd Mate
	P6	GND		1 st Mate	2 nd Mate
	P7	V5	5V Power, Pre-charge	1 st Mate	2 nd Mate
	P8	V5	5V Power	2 nd Mate	3 rd Mate
	P9	V5	5V Power	2 nd Mate	3 rd Mate
	P10	GND		1 st Mate	2 nd Mate

到了SATA 3.2，管脚3用来做DevSlp控制，如表8-2所示。

表8-2 SATA 3.2管脚定义—管脚3用于DevSlp

	名称	类型	描述	线缆形式	背板形式
信号部分	S1	GND	差分信号组 A	1 st Mate	2 nd Mate
	S2	A+		2 nd Mate	3 rd Mate
	S3	A-		2 nd Mate	3 rd Mate
	S4	GND	差分信号组 B	1 st Mate	2 nd Mate
	S5	B-		2 nd Mate	3 rd Mate
	S6	B+		2 nd Mate	3 rd Mate
	S7	GND		1 st Mate	2 nd Mate
电源部分	P1	Retired		2 nd Mate	3 rd Mate
	P2	Retired		2 nd Mate	3 rd Mate
	P3	DEVSLP	进 / 出 DevSleep	1 st Mate	2 nd Mate
	P4	GND		1 st Mate	1 st Mate
	P5	GND		1 st Mate	2 nd Mate
	P6	GND		1 st Mate	2 nd Mate
	P7	V5	5V Power, Pre-charge	1 st Mate	2 nd Mate
	P8	V5	5V Power	2 nd Mate	3 rd Mate
	P9	V5	5V Power	2 nd Mate	3 rd Mate
	P10	GND		1 st Mate	2 nd Mate

DevSlp注意事项:

·主机和设备都必须支持该功能才可以工作，主机置位DevSlp信号前需要确保：OOB结束以后通过Identify Device命令获得的设备回复支持DevSlp。

·主机已经通过Set Feature命令打开设备的DevSlp。

·没有还没执行完的命令。

主机置位DevSlp时:

·MDAT（Minimum Device Sleep Assertion Time：主机要么不弄，要弄必须保持置位状态≥10ms（或者是Identify Device Data log里规定的时间）；

·DMDT（DEVSLP Minimum Detection Time）：设备在DevSlp置位后需要在10us内检测到；

·主机和设备可以把PHY和其他东西（PLL、时钟、闪存芯片）都关掉；

·DevSlp置位后，主机和设备双方都不可以主动通过PHY进行通信，即使一方通信，另一方也不准搭理。

退出DevSlp时：

·DETO（Device Sleep Exit Timeout）：设备必须在20ms（或者Identify Device Data log里规定的时间）内检测到OOB信号；

·双方使用COMWAKE或者COMRESET/COMINIT重新建立连接。

图8-5展现了DevSlp的进入/退出流程。

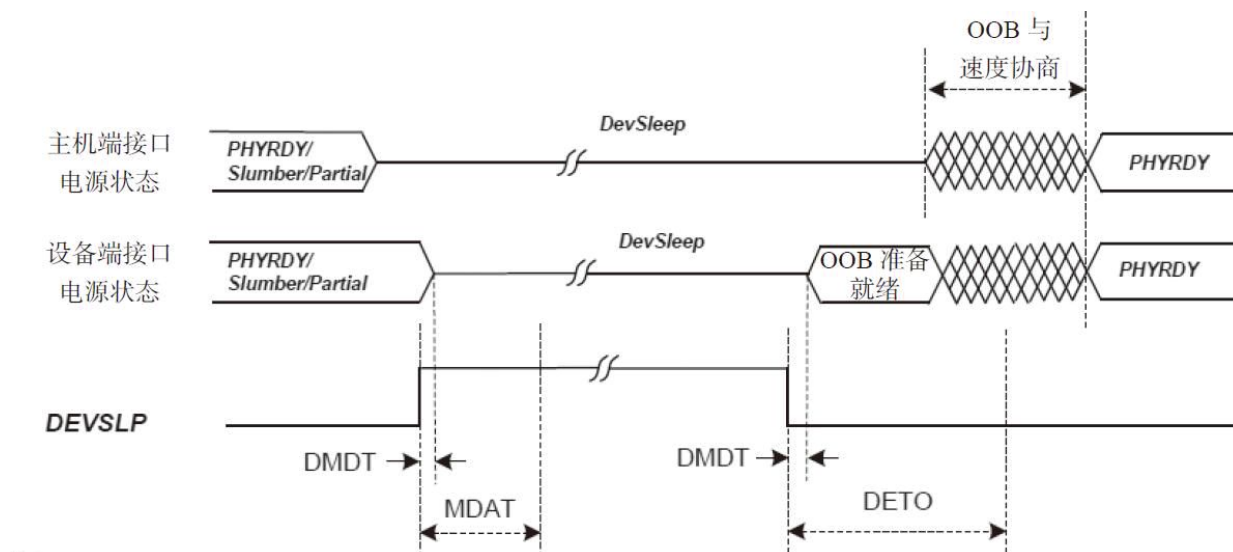


图8-5 DEVSLP过程示意图

8.3 SATA终极省电模式RTD3

DevSlp那么好，主机却仍不满足，因为DevSlp虽然功耗小，恢复时间也还行，但是进入DevSlp的时候Vcc还在，这样还是会有功耗，进而得寸进尺地要求设备在长期Idle后要把Power完全关掉。

在两者的博弈当中，SATA SSD作为设备永远是弱势的一方，所以需要考虑如何满足这个要求：在主机也就是系统处于S0的情况下，如何让SATA SSD进入D3Cold状态，这个就是Runtime D3，简称RTD3。

了解以下概念能够更好地理解RTD3。

ACPI规定的Device Power State:

·D0：设备处于工作状态，所有功能可用，功耗最高，所有设备都必须支持；

·D0active：设备完成配置，随时准备工作；

·D1和D2是介于D3和D0之间的中间状态，D1比D2消耗更多的电能，保存更多的设备上下文，D1和D2是可选的，很多设备都没有实现这两个状态；

·D3Hot：设备进入D3，Vcc还在，设备可被软件枚举；

·D3Cold：设备完全切断电源，重新上电时系统需要重新初始化设备。

表8-3列出了不同电源状态下功耗，保留设备上下文以及驱动恢复的具体信息。

表8-3 不同电源状态的具体信息

设备状态	功耗	保留设备上下文	驱动恢复
D0 – Fully On	按需	全部	无
D1	D0>D1>D2>D3hot>D3	>D2	<D2

(续)

设备状态	功耗	保留设备上下文	驱动恢复
D2	D0>D1>D2>D3hot>D3	<D1	>D1
D3 Hot	D0>D1>D2>D3hot>D3	可选	重新初始化并加载驱动
D3 Cold	0	无	重新初始化并加载驱动

图8-6展现了这些状态之间的转换关系。

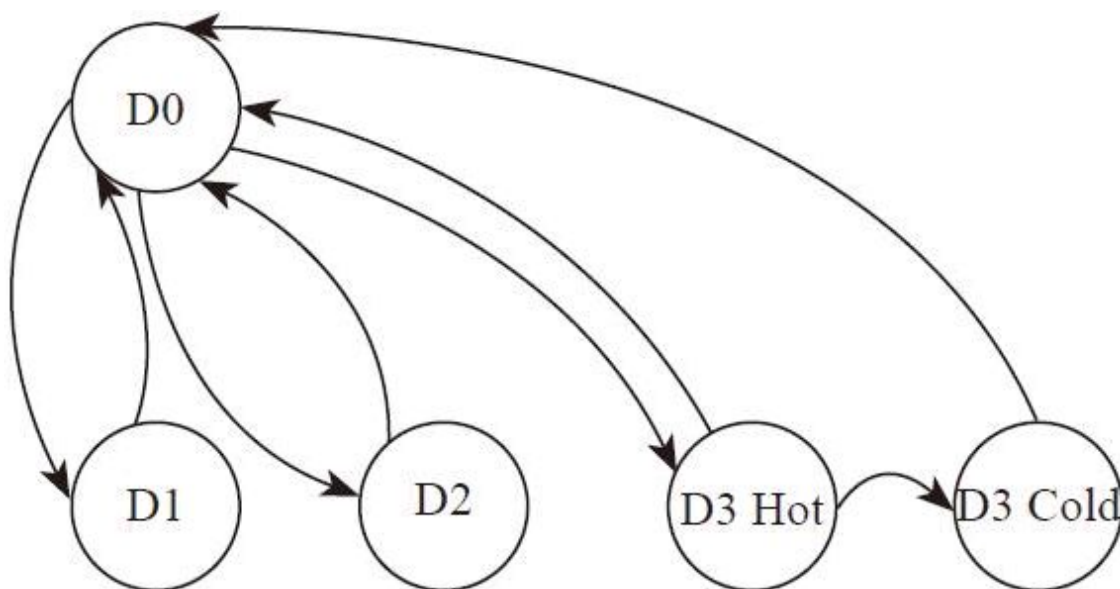


图8-6 设备Power State转换关系

Partial和Slumber模式都是只针对SATA链路，而D State是针对整个SSD，如图8-7所示。

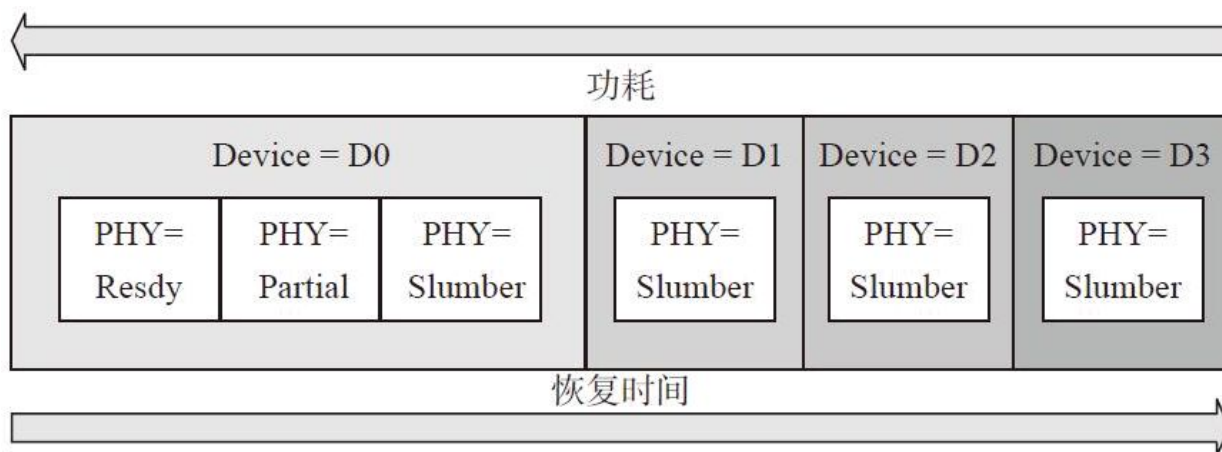


图8-7 Partial和Slumber模式与不同电源状态之间的对应关系

系统电源状态（SATA SSD作为系统盘）：

·S0：工作模式，操作系统可以管理SATA SSD的电源状态，D0或者D3都可以；

·S1：低唤醒延迟的状态，系统上下文不会丢失（CPU和芯片组），硬件负责维持所有的系统上下文；

·S2：与S1相似，不同的是处理器和系统Cache上下文会丢失（操作系统负责维护Cache和处理器上下文），收到唤醒要求后，从处理器的复位向量开始执行；

·S3：睡眠模式（Sleep），CPU不运行指令，SATA SSD断电，除了内存之外的所有上下文都会丢失，硬件会保存一部分处理器和L2Cache配置上下文，从处理器的复位向量开始执行；

·S4：休眠模式（Hibernation），CPU不运行指令，SATA SSD断电，内存内容写入SSD，所有的系统上下文都会丢失，操作系统负责上下文的保存与恢复；

·S5：Soft off state，与S4相似，但操作系统不会保存和恢复系统上下文，消耗很少的电，可通过鼠标键盘等设备唤醒。

注意事项：

1) 需要主板芯片组、操作系统和SSD三方都支持，RTD3才能工作；

2) SSD可以支持D3Hot或者D3Cold状态；

3) SSD不需要做硬件改动，厂家自行优化，保证从D3回到D0的时间不能长到能被用户察觉；

4) RTD3和DevSlp功能完全独立，可以互为补充，更好地服务主机；

5) 操作系统通过发送Standby Immediately命令通知SSD把脏数据写入闪存，然后把SSD切到RTD3状态；

6) 与Partial、Slumber和DevSlp不同，进了RTD3以后，SSD上之前主机做的设置全都没有了，重新上电的时候主机需要通过以下命令恢复之前的设置：

- SET FEATURES
- DEVICE CONFIGURATION FREEZE LOCK
- SET MAX FREEZE LOCK
- SET MAX ADDRESS (If V_V attribute is not used)
- SECURITY FREEZE LOCK

表8-4显示了不同省电模式功耗、转换时间、恢复时延的对比。可见，使用了RTD3后，功耗为0，进入时间为1.5s，退出时间为0.6s。

表8-4 不同的省电模式功耗，转换时间，恢复时延对比

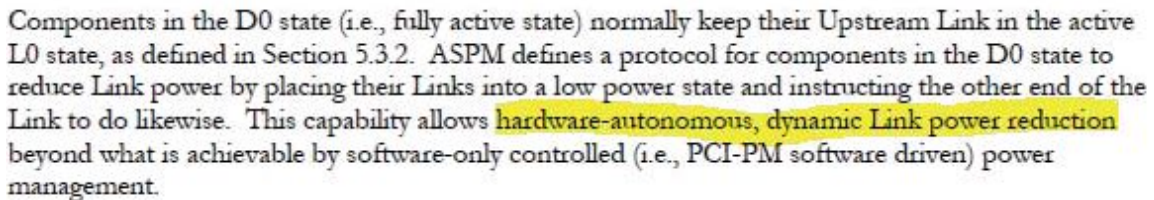
设备（链路）状态	功耗（mW）	转换时间（s）	恢复时延（s）
工作（Ready）	>1000	0	0
空闲（Partial）	100	10^{-6}	10^{-4}
空闲（Slumber）	50	10^{-3}	0.01
空闲（DEVSLP）	5	0.02	0.02
关闭 – RTD3（n/a）	0	1.5	0.6

RTD3不是SATA设备的专利，SATA HBA也可以。

8.4 PCIe省电模式ASPM

现在消费级笔记本里搭载SSD已经越来越多，而搭载PCIe SSD也正在成为趋势。

做消费级SSD的厂商那么多，但常见的PCIe主控就那么几款：SMI 2260、PS5007-E7、88SS1093和88NV1140（三星这个巨鳄就不提了）。这些主控都支持一个叫ASPM的功能，ASPM的全称是：Active State Power Management。其实Active前面还缺省了两个词，Hardware Initiated——ASPM的第一个重要概念：这是HW也就是主控自己触发的，不需要主机或者固件干涉，如图8-8中的高亮部分。



Components in the D0 state (i.e., fully active state) normally keep their Upstream Link in the active L0 state, as defined in Section 5.3.2. ASPM defines a protocol for components in the D0 state to reduce Link power by placing their Links into a low power state and instructing the other end of the Link to do likewise. This capability allows hardware-autonomous, dynamic Link power reduction beyond what is achievable by software-only controlled (i.e., PCI-PM software driven) power management.

图8-8 PCIe协议对ASPM的定义截图

ASPM让PCIe SSD在某种情况下，能够从工作模式（D0状态）通过把自身PCIe链路切换到低功耗模式，并且通知对方也这么干，从而达到降低整条链路功耗的目的。

ASPM定义的低功耗模式有两种：L0s和L1（见图8-9深色部分）。

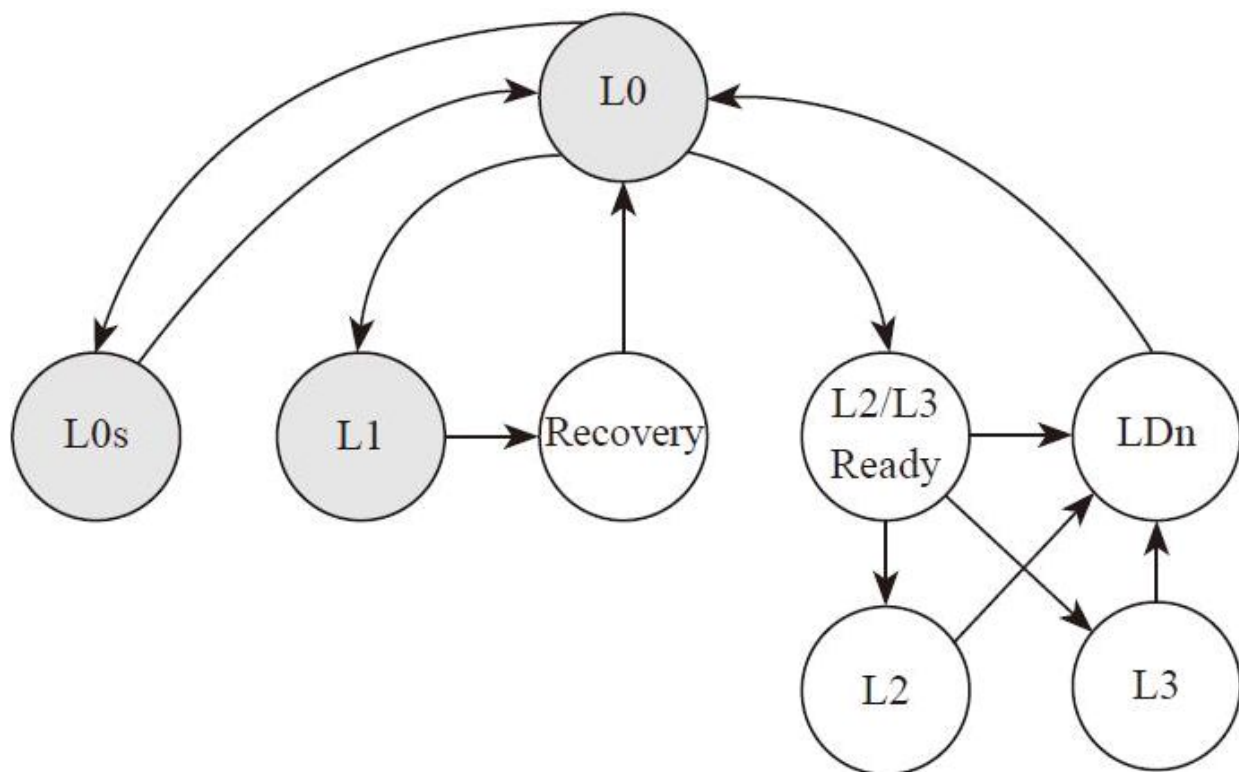


图8-9 PCIe链路状态转换关系

图8-9中所示各状态的定义如下：

- L0：正常工作状态；
- L0s：低功耗模式，恢复时间短；
- L1：更低功耗模式，恢复时间较长；
- L2/L3Ready：断电前的过渡状态；
- L2：链路处于辅助供电模式，极省电；
- L3：链路完全没电，功耗为0；
- LDn：刚上电，LTSSM还未完成前链路所处状态。

要看一款SSD是否支持ASPM，你需要查看它的Link Capabilities Register（链路能力寄存器）的bit 11: 0（见图8-10）。

Bit11: 10（只读属性）中对ASPM支持的具体定义如下：

- 00b: 保留。
- 01b: 支持L0s。
- 10b: 保留。
- 11b: 支持L0s和L1。



图8-10 链路能力寄存器

仅仅支持是没有用的，还需要把开关打开，查看链路控制寄存器的bit1: 0，如图8-11所示。



图8-11 链路控制寄存器

Bit1: 0（可读写属性）中对ASPM控制的具体定义如下：

- 00b: 禁用。

- 01b: L0s使能。
- 10b: L1使能。
- 11b: L0s和L1均使能。

关于ASPM控制，PCIe协议手册中这样描述：

- L0s，即使RC和EP某一方的L0s是关闭的，如果对方要求进入L0s，本方也要跟着进；
- L1，打开时必须先开RC，再开EP，关掉时必须先关EP再关RC；
- 如果RC和EP都支持ASPM L1，那必须把EP的L1打开。

L0s的流程比较简单：

进入：

- SSD可以直接在Tx lane上启动进入L0s；
- 如果SSD的Tx的L0s被关闭，Rx还是接受来自RC的L0s请求。

退出：

- 双方都可以启动退出流程；
- 发送FTS（Fast Training Sequence），然后发送一个SKP，对方借此恢复bit和symbol lock。

进入L1的流程相对复杂一点，如表8-5所示。

表8-5 PCIe ASPM L1进入流程

步骤	EP	RC
1	停止接收后续的 TLP	—
2	确认发送的最后一个 TLP 已经收到对方的 ACK（确保 Replay Buffer 是空的）	—
3	确认 FC Credit 足够（可以满足一个最大长度的传输）	—
4	持续发送 PM_Active_State_Request L1 给 RC，直到 RC 回复 PM_Request_ACK	—
5	—	收到 PM_Active_State_Request L1
6	—	停止接收后续的 TLP
7	—	确认发送的最后一个 TLP 已经收到对方的 ACK（确保 Replay Buffer 是空的）
8	—	确认 FC Credit 足够（可以满足一个最长的传输）
9	—	持续发送 PM_Request_ACK，直到 EP 发送 Electrical Idle
10	收到 PM_Request_ACK，Disable TLP/DLLP 包的传输	—
11	发送 Electrical Idle，进入 L1	—
12	—	收到 Electrical Idle，Disable TLP/DLLP 包的传输
13	—	进入 L1

退出：

- 双方都可以启动退出流程；
- 不是发送FTS，而是重新进行Link Training；
- 唤醒发起方，发送TS1，走LTSSM的恢复步骤重新建立连接。

最后说一下链路控制寄存器的bit7，Extended Sync。

Link Control Register（链路控制寄存器）

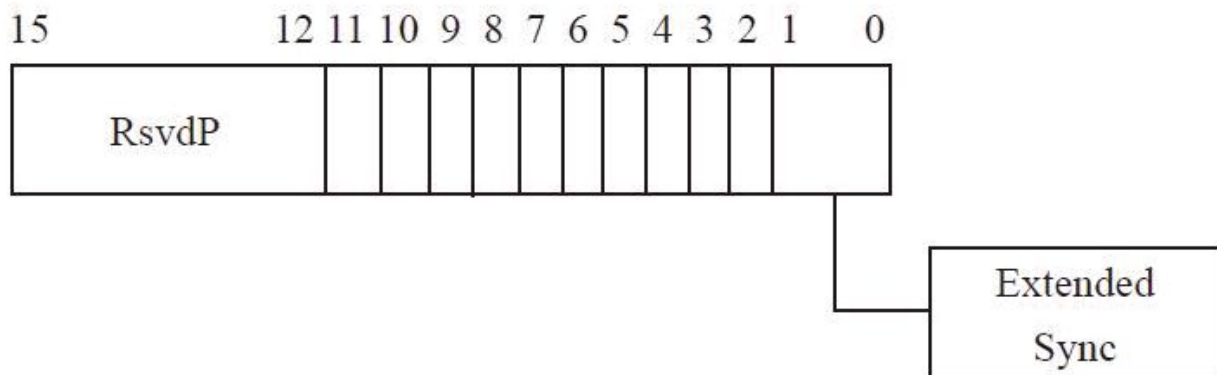


图8-12 链路控制寄存器定义

Extended Sync是一个神奇的bit，置上以后从L0s和L1退出时，设备会发超多的FTS和TS1，最终让双方“握手”成功（见图8-13）。

Extended Sync – When Set, this bit forces the transmission of additional Ordered Sets when exiting the L0s state (see Section 4.2.4.5) and when in the Recovery state (see Section 4.2.6.4.1). This mode provides external devices (e.g., logic analyzers) monitoring the Link time to achieve bit and Symbol lock before the Link enters the L0 state and resumes communication.

For multi-Function devices if any Function has this bit Set, then the component must transmit the additional Ordered Sets when exiting L0s.

Default value for this bit is 0b.

图8-13 Extended Sync定义

这个模式是当链路中有额外设备（例如PCIe分析仪）时，为保证能够正常达到bit和symbol lock用的。

但是遇到ASPM L1回不来或者开机找不到PCIe设备的情况，也可以通过设置这个bit收集更多的参考数据。

8.5 PCIe其他省电模式

PCIe链路L2状态下，所有的时钟和电源全部关闭，能够保证最大的省电效果，但同时，L2的退出时间相应也增加了很多，达到了毫秒级别。这样的时间在很多应用场景下是无法接受的。

要比L1更省电，比L2时间更短，PCI-SIG顺理成章地弄出了两个新的ASPM Sub状态：L1.1和L1.2。想要使用L1.1和L1.2，RC和EP都必须支持并打开这个功能，同时还必须支持CLKREQ#信号。

在L1.1和L1.2模式下，PCIe设备内部的PLL处于关闭状态，参考时钟也不保留，发送和接收模块同样关闭，不需要像L1状态下那样去侦测Electrical Idle。

L1.1和L1.2的区别在于，L1.1状态下Common Mode Voltage仍然打开，而L1.2下会将之关闭。因为Common Mode Voltage恢复需要时间，L1.2的退出时间相对比L1.1长一些。

从表8-6中可以看到L1、L1.1、L1.2功耗和时延对比。

表8-6 L1、L1.1、L1.2功耗和时延对比

电源状态		状态（开 / 关）			目标	
链路状态	PHY/PIPE	PLL	接收端 / 发送端	Common Mode Keepers	1 条 Lane 功耗	退出时间
L1	P1	开 / 关	关 / 空闲	开	20's of mW 10's of mW	< 5 μ s (retrain) < 20 μ s(PLL Off)
L1.1	P1.1	关	关	开	< 500 μ W	< 20 μ s
L1.2	P1.2	关	关	关	< 10 μ W	< 70 μ s

使用L1.1/L1.2后，功耗从毫瓦级别降到了微瓦级别，相比之下时延的增加完全在可接受的范围内。

8.6 NVMe动态电源管理

PMC（MicroSemi）管自己的PCIe SSD主控叫Flashtec NVMe控制器，一共有4款：PM8602NVMe1016、PM8604NVMe1032、PM8607NVMe2016和PM8609NVMe2032。其实主要是有两款，10xx和20xx，分别支持16和32通道。

在看官网的介绍时，有这么一段话介绍电源管理优化的，如图8-14所示。

Microsemi's NVMe1032 has been optimized for power savings using a combination of architectural and semiconductor design techniques. Emphasis has been given not only to absolute power consumption, but also to advanced power management features, including, automatic idling of processor cores and autonomous power reduction capabilities. The NVMe1032 allows the platform to provide power and performance objectives through the Enterprise NVM Express dynamic power management interface, allowing firmware to effectively manage power and performance.

图8-14 Microsemi官网电源管理优化介绍截图

里面提到一个术语，叫作Enterprise NVM Express dynamic power management interface。企业、动态、电源管理、接口，瞬间觉得有点高大上。

第一个问题，什么是Enterprise NVMe？

Bing了半天搜不到。问了一圈周围的高人，也都说没听过，基本确认加上Enterprise这个前缀是为了提升档次。

第二个问题，NVMe电源管理都包括什么？

然后，查到图8-15所示的这个路线图。

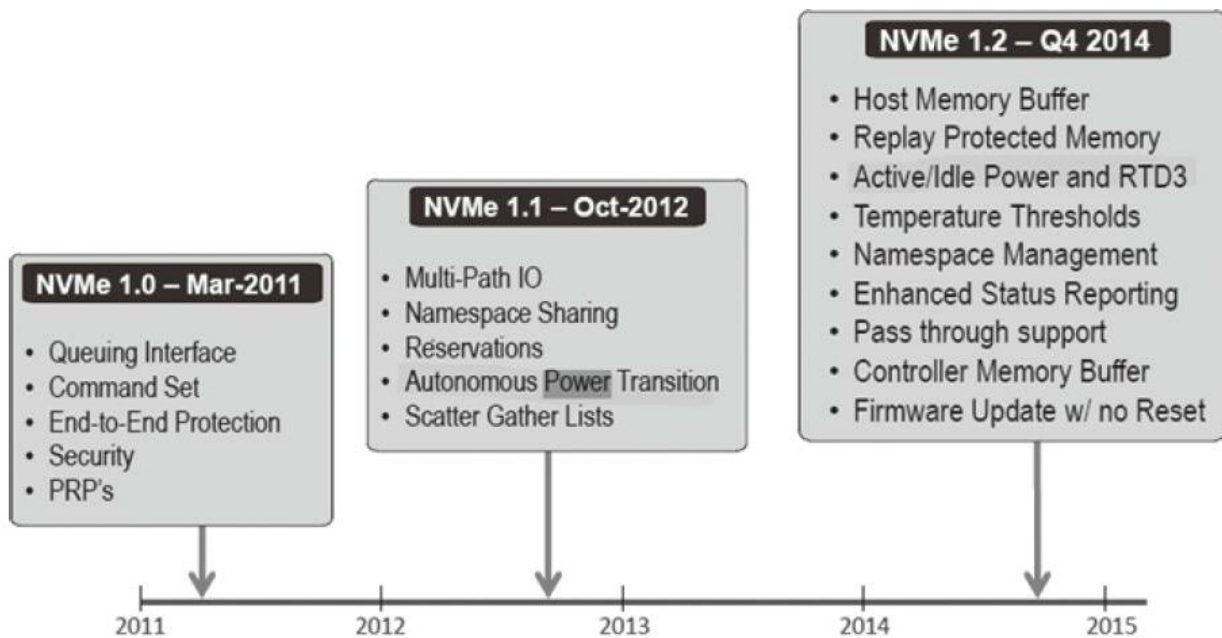


图8-15 NVMe路线图

路线图中电源管理相关的内容包括：

- Autonomous Power Transition;
- Active/Idle Power;
- RTD3。

第三个疑问，Dynamic Interface是什么？

翻NVMe协议手册（NVMe 1.2a），看图8-16中的高亮部分，PMC说的动态接口应该就是对NVMe电源管理这部分。

8.4 Power Management

The power management capability allows the host to manage NVM subsystem power statically or dynamically. Static power management consists of the host determining the maximum power that may be allocated to an NVM subsystem and setting the NVM Express power state to one that consumes this amount of power or less. **Dynamic power management is illustrated in Figure 217 and consists of the host modifying the NVM Express power state to best satisfy changing power and performance objectives.** This power management mechanism is meant to complement and not replace autonomous power management performed by a controller.

图8-16 NVMe 1.2a Section 8.4

NVMe协议里给出了动态电源管理的框图（见图8-17）。

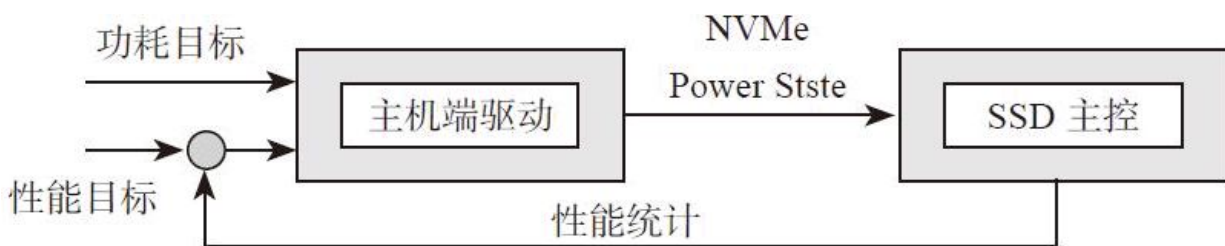


图8-17 NVMe动态电源管理逻辑图

功耗目标和性能目标作为系统应用层面的输入，发送给主机端的NVMe驱动。

NVMe Power State: NVMe规定（Identify Controller Data Structure）最多支持32个Power State Descriptor（电源状态描述符），如表8-7所示。其中Power State Descriptor 0（0号电源状态描述符）是必须支持的，其他都是可选。当然，如果只支持一个，也别用什么动态管理了。

表8-7 NVMe电源状态描述符

电源状态描述符		
2079:2048	强制	电源状态描述符 0
2111:20800	可选	电源状态描述符 1
.....
3039:3008	可选	电源状态描述符 30
3071:3040	可选	电源状态描述符 31

一个Power State Descriptor的具体数据结构为32Byte，定义了该电源状态下的各种属性，具体各位定义如下：

- 255: 184: 保留；
- 183: 182: Active Power Scale，工作模式功耗粒度；
- 181: 179: 保留；
- 178: 176: Active Power Workload，用于计算工作模式功耗的工作负载；
- 175: 160: Active Power，工作模式平均功耗，这个值乘以工作模式功耗粒度，就是工作情况下的实际功耗值；

- 159: 152: 保留;
- 151: 150: **Idle Power Scale**, 空闲模式功耗粒度;
- 149: 144: 保留;
- 143: 128: **Idle Power**, 空闲模式平均功耗, 这个值乘以空闲模式功耗粒度, 就是空闲情况下的实际功耗值;
- 127: 125: 保留;
- 124: 120: **Relative Write Latency**, 写延迟, 值越小代表延迟越低 (这个值的分级级数必须小于主控支持的电源状态数量, 主控不能一边只支持5个电源状态, 一边又支持10种写入延迟);
- 119: 117: 保留;
- 116: 112: **Relative Write Throughput**, 写入吞吐量, 值越小代表吞吐量越高 (这个值的分级级数同样必须小于主控支持的电源状态数量);
- 111: 109: 保留;
- 108: 104: **Relative Read Latency**, 读延迟, 值越小代表延迟越低;
- 103: 101: 保留;
- 100: 96: **Relative Read Throughput**, 读取吞吐量, 值越小代表吞吐量越高;
- 95: 64: **Exit Latency**, 退出该电源状态的时间 (微秒级);
- 63: 32: **Entry Latency**, 进入该电源状态的时间 (微秒级);
- 31: 26: 保留;
- 25: **Non-Operational State**, 为“0”代表在这个电源状态主控可以处理IO, 为“1”代表在这个电源状态主控不能处理IO;

- 24: Max Power Scale, 最大负载功耗粒度;
- 23: 16: 保留;
- 15: 00: MaximumPower, 最大负载功耗, 这个值乘以最大负载功耗粒度, 就是最大负载情况下的实际功耗值。

主机和主控之间, 就通过对这些值的修改, 实现如图8-18所示的沟通。

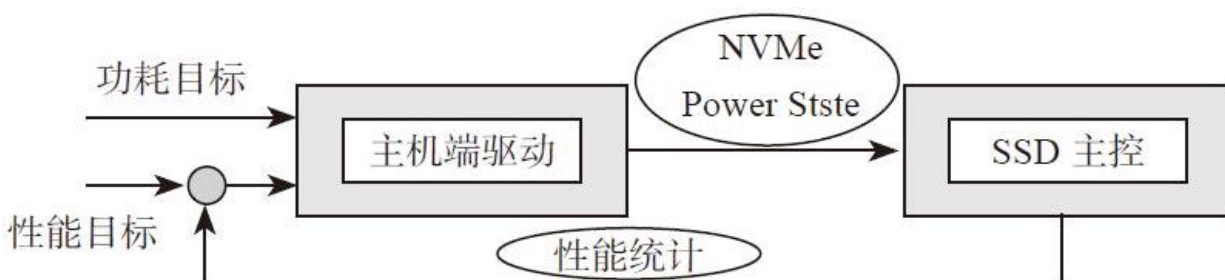


图8-18 主机和控制器之间交流电源状态和性能信息

同时主机通过Entry Latency和Exit Latency两个值, 做出决策是否进入, 何时进入某个电源状态。

第四个问题, 主机的具体操作都有哪些?

- 1) 主机给主控发个Identify Controller命令, 主控会回复一个4K的数据包。
- 2) 主机解析字节263获知主控支持的电源状态的数量。
- 3) 主机解析字节2079: 3140获知每个电源状态下主控的具体属性。

例如主控可以支持四种电源状态:

- PS0: 均衡模式 (平衡考虑功耗、读写性能、延迟、但每个都不突出);
- PS1: OLTP模式, 大量随机小IO (要求低延迟);

- PS2：视频模式，大小连续大IO（要求高吞吐量）；
- PS3：绿色模式，低能耗。

NVMe协议里也给出了不同电源状态的示例，如表8-8所示。

表8-8 不同电源状态对比

电源状态	最大负载功耗（W）	进入时间（μs）	退出时间（μs）	读吞吐量	读延迟	写吞吐量	写延迟
0	25	5	5	0	0	0	0
1	18	5	7	0	0	1	0
2	18	5	8	1	0	0	0
3	15	20	15	2	0	2	0
4	10	20	30	1	1	3	0
5	8	50	50	2	2	4	0
6	5	20	5000	4	3	5	1

4）主机根据正在运行的应用（例如邮箱服务、数据库服务、视频服务和股票交易服务等）选择主控合适的电源状态，具体实现是通过Set Feature命令（Feature ID 0x02），在DW 11的Bit 04：00，如表8-9和表8-10所示。

表8-9 Set Feature命令中功耗管理定义

功能 ID	描述	功能 ID	描述
00h	保留	04h	温度阈值
01h	仲裁命令	05h	错误恢复
02h	电源管理
03h	LBA 范围类型		

表8-10 功耗管理命令DWORD11定义

位	描述
31:08	保留
07:05	负载类型：指明使用工作负载的类型，用于优化性能
04:00	电源状态：指明设备接下来准备转入的电源状态

5）同理，主机也可以通过Get Feature命令来获知当前主控所处的电源状态，如图8-19所示。

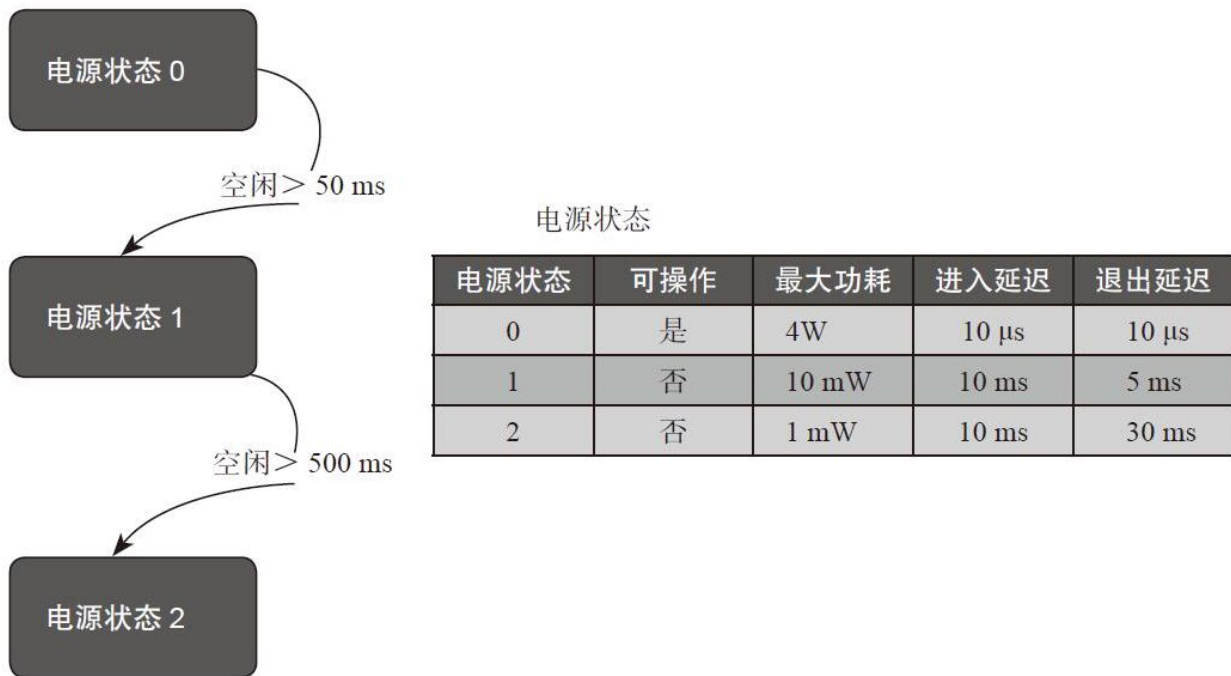


图8-19 功耗状态跳转示例

设几个状态跳来跳去容易，而具体的跳转策略要结合当前IO模式、功耗要求和Enter/Exit延迟来决定跳不跳，何时跳，跳哪里，这才是核心价值。这块没法继续看手册找答案了，如果有条件，抓几个典型应用场景切换时的PCIe trace，那应该可以发现部分策略，另外可以读到支持的Power State Descriptor，可能也能反推出一些策略的考虑点。

8.7 Power Domain

对于一块SSD，尤其是用于消费级的SSD，为什么功耗这么重要？因为对于消费级来说最大的市场是OEM，而OEM市场里笔记本市场搭载已经是大势所趋！

笔记本与台式机相比的两大特点：

- 用电池。
- 结构相对紧凑。

要求电池寿命长；要求SSD功耗低，结构紧凑；要求SSD体积小，发热少。这都意味着SSD必须控制功耗。

我们以SMI的某款主控为例，看看它是如何进行功耗控制的，如表8-11所示。

表8-11 某SMI主控功耗控制

NVMe 电源状态	PCIe 链路状态	工作 / 空闲	功耗	退出时延
PS0	L0/L0s/L1	工作	100%	无
PS1	L0/L0s/L1	工作	75%	极短
PS2	L0/L0s/L1	工作	40%	极短
PS3	L1/L1.1/L1.2	空闲	低	适中
PS4	L1.2	空闲	极低	长

又看到了NVMe Power State这个熟悉的配方，没错——跟PMC的做法差不多：

- 提前在固件中定义好一系列不同的电源状态，不同的电源状态配置PCIe链路状态、SSD Active/Idle、功耗比、退出时延等；
- 通过NVMe下发切换电源状态的指令。

从功耗这列可以看到，功耗可以降低到正常工作状态下的40%，甚至更低，仅靠调整PCIe Link State是没办法省这么多电的。

这样就引入了Power Domain的概念，如图8-20所示。

从图8-20中可以看到，主控把芯片内部的模块划分成了几个部分，学名叫Power Domain，简称PD。

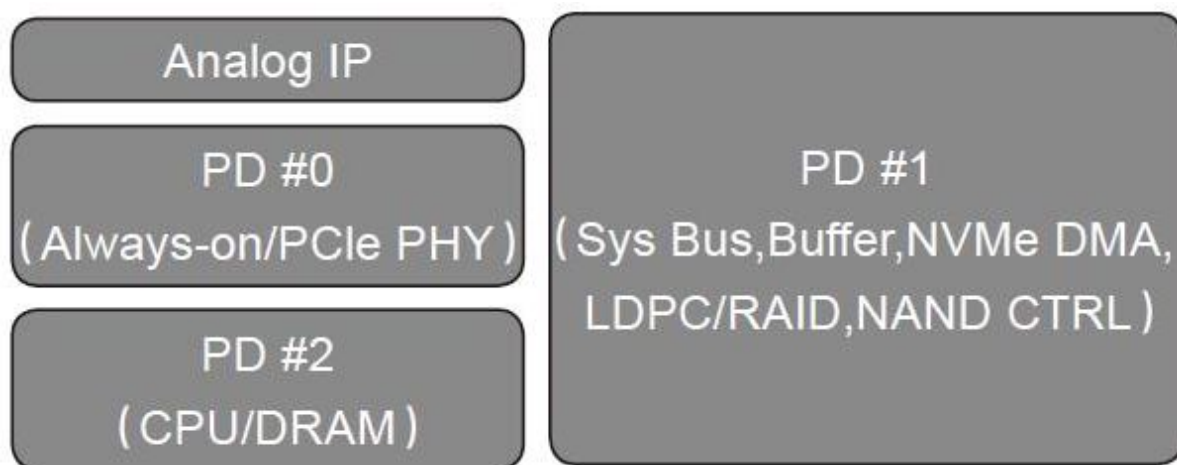


图8-20 SMI主控芯片模块划分

- PD#0: Always-on/PCIe PHY;
- PD#1: 最大的一部分，包括Sys Bus、Buffer、NVMe DMA、LDPC/RAID、NAND CTRL;
- PD#2: CPU/DRAM。

整个节能逻辑的大致演绎如下：

- 1) 主机一段时间没有读写，触发SSD的PCIe链路进入ASPM，退出延迟非常短；
- 2) 主机继续Idle，PCIe链路进入ASPM Substate，SSD仍处于工作模式，退出延迟也很短；
- 3) 主机继续Idle，主控操作PD#1（关闭NVMe模块、各级FIFO、ECC模块、闪存控制器等），SSD进入Idle Mode，退出延迟明显延长；
- 4) 主机继续Idle，主控操作PD#2，将CPU进入睡眠模式，DRAM进入Self Refresh模式，进入最高节能模式，退出延迟最长；

最后，为了更好地控制发热，主控会设置一个温度阈值，当芯片温度接近阈值时，主动降低时钟频率，使温度降低。等温度回到指定范围，再把时钟调回正常工作频率，如图8-21所示。

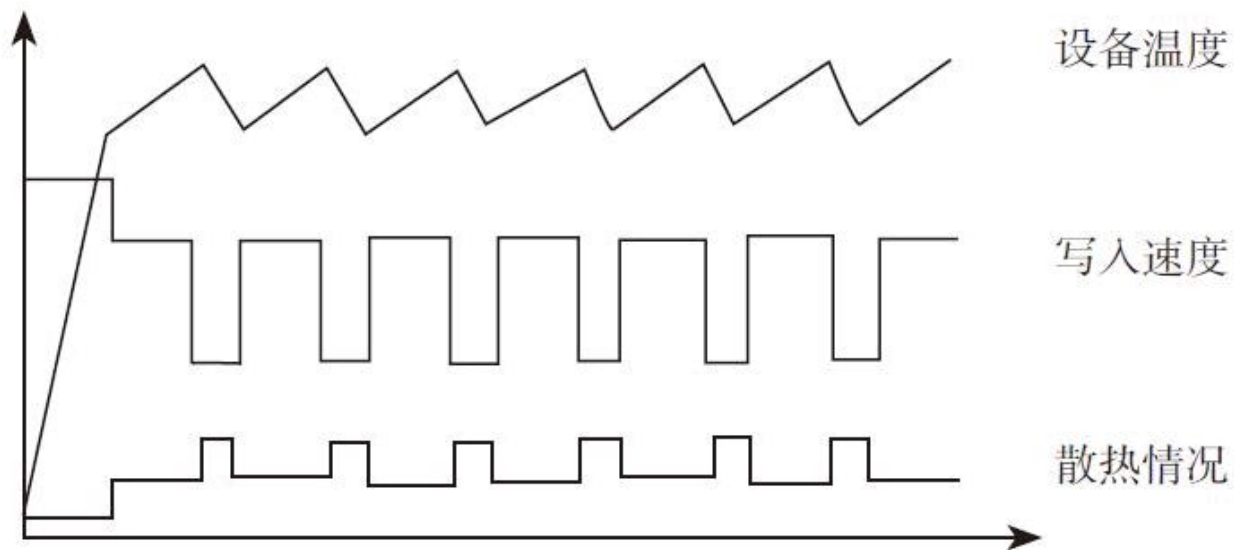


图8-21 SSD主控温度调节波形图

第9章 ECC原理

我们知道，所有型号的闪存都无法保证存储的数据会永久稳定，这时候就需要ECC（纠错码）去给闪存纠错。ECC能力的强弱直接影响到SSD的使用寿命和可靠性。本章将简单介绍ECC的基本原理和目前最主流的ECC算法——LDPC。

9.1 信号和噪声

噪声信号充斥着整个世界，不只包括打电话时对方声嘶力竭的喊声，也包括还钱时手抖多按的一个0，甚至在生物学领域，基因对的复制偏差、癌细胞的产生、意外突破橡胶屏障的新生命都可以划入噪声信号的范畴。凡是有信息传递的地方就有噪声。我们唯一能做的是，把噪声限制在一定大小的笼子里。

如何建造这样一个笼子？我们看一下历史的经验。

场景是，蛋蛋每天坐地铁都会邂逅一个美丽的女孩。两人日久相熟，经常相视一笑，却默然无语。转眼间，蛋蛋就要离开这个城市，他决定勇敢地表白。

表白的地点还是那一班地铁。唯一的困难是地铁太吵了，女神能够准确无误地接收到蛋蛋爱的呼唤吗？这难不倒蛋蛋，他采取了以下策略。

- 1) 扩音器一个。
- 2) 每个字清晰地说三遍。
- 3) 结尾用手比画一个爱心出来。

利用扩音器可以改善有效信号和噪声的强度比，为女神准确地接收做了基础建设。每个字说三遍，增加了信息的冗余，即使有少量字没有听清，也不影响表达的内容。结尾一个爱心的手势，增加对关键信息的保护，借助大家都懂的意象，盖上爱的印章。

聪明的蛋蛋揭示了长久以来我们传播信息的诀窍。增强信号和噪声的强度比，增加信号冗余。前者不在此讨论，我们只考虑在不用扬声器的情况下，如何尽量准确地传递信息。

实际通信中，我们用**information bits**表示有效信息长度，**channel use**表示实际通信中传输的信息长度。定义：

$$\text{Code rate} = (\text{information bits}) / (\text{channel use})$$

举个例子，因为每个字说三遍，所以蛋蛋采用的Code rate为1/3。

Code rate可以反映冗余程度。Code rate越高，冗余越小，反之冗余越大。Shannon揭示了，每一种实际的信息传输通道都有一个参数C，如果Code rate < C，有效信息传递的错误率可以在理论上趋近于0。但是如何趋近于0，就是纠错编码（Error correction code）要做的事情了。

我们后续的讨论只限制在二进制的世界，即所有的信息都是用二进制表示。

9.2 通信系统模型

所有的信息传播都少不了通信系统，一个完整的通信系统模型，信息由信息源产生，由发送器发送出信号，通过包含噪声的信号传输通道（Channel，信道）、到达接收器，再由接收器提取出信息发送到目的地。

整个框图如图9-1所示。

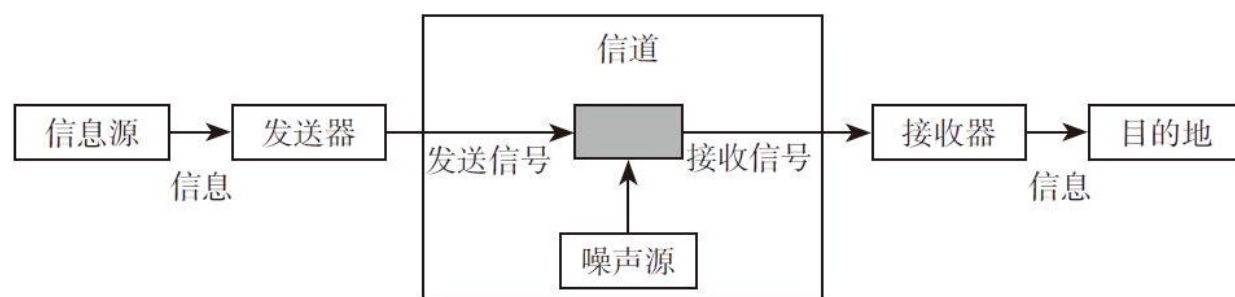


图9-1 通信系统框图

回到蛋蛋跟女神表白的例子；蛋蛋心中所想就是信息源；发送器是神经和肌肉控制的嗓子；声音就是信号；嘈杂的车厢就是Channel；女神的耳朵就是接收器，最终信息反映到女神大脑中。

SSD存入和读出信息也是一个通信系统。信息是用户写入的原始数据，经过SSD后端的发送器处理后转化为闪存的program，信号就是闪存上存储的电荷，电荷存储时会有自身泄露并在读的过程中受到周围电荷的影响，这是内存的信道特性，最后数据通过SSD后端的读取接收器完成读取过程。

在二进制编码的系统中，有两种常见的Channel模型——BSC（Binary Symmetric Channel，二进制对称信道）和BEC（Binary Erasure Channel，二进制擦除信道）。一句话区分BSC和BEC：BSC出错（接收者收到的0不一定是0，可能发送者发送的是1；同样，收到的1不一定是1，可能发送者发送的是0）；BEC丢bit（接收者如果收到0（1），那么发送者发送的肯定是0（1）；如果传输发生错误，接收者则接收不到信息）。

BSC模型如图9-2所示。

二进制信号由0、1组成，由于Channel噪声的影响，0、1各有相同的概率 p 翻转，即0变1，1变0。信号仍然保持不变的概率为 $1-p$ 。

例如一串二进制信号，在经过BSC模型后，原始信号“101001101010”变为“111001111000”。

BEC模型如图9-3所示。

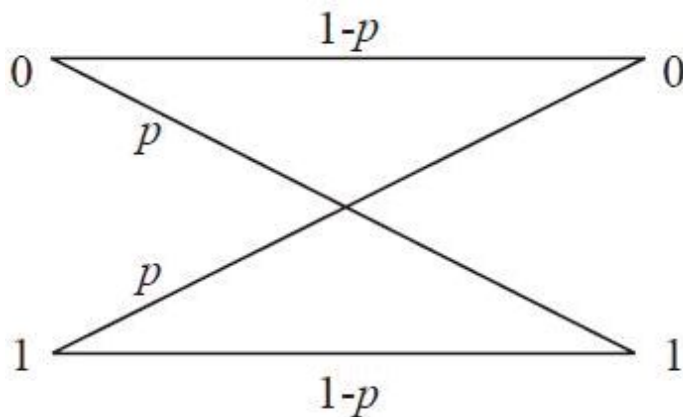


图9-2 BSC模型

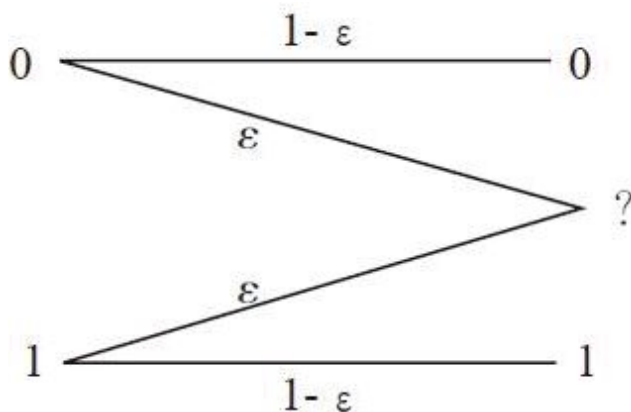


图9-3 BEC模型

BEC模型认为在信号传输中，无论是0还是1都有一定概率变为一个无法识别的状态。

例如一串二进制信号，在经过BEC模型后，原始信号“101001101010”变为“1x10011x10x0”（x表示未知状态）。

对于SSD里的Channel模型一般采用BSC，即认为闪存信号发生了一定概率的位翻转（bit-flip）。

为了使得信息从源头（source）在经过噪声的信道后能够准确到达目的地，我们要对信息进行编码，通过增加冗余的方式保护信息。

基本流程如图9-4所示，具体说明如下。

Source发出的信息可用k bit的信息 x 表示，经过编码器（Encoder）转化为n bit信号 c 。这个从k bit到n bit的过程叫编码过程，也是添加冗余的过程。信号 c 的所有集合叫编码集合。

发送器把信号发送出去，经过Channel后，接收器收到信号n bit信号 y ，经过解码器（Decoder）转成k bit信息 \hat{x} ；这个过程是解码过程；如图9-4所示。

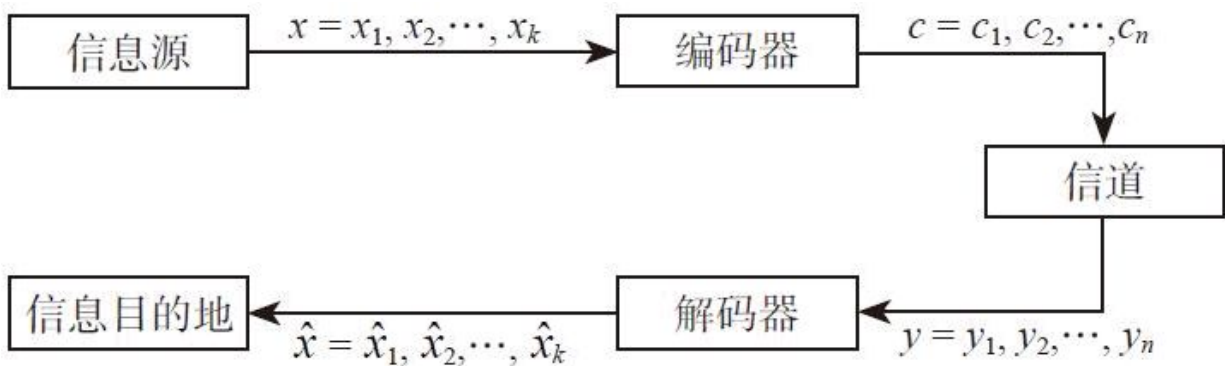


图9-4 信息编码解码过程

9.3 纠错编码的基本思想

纠错编码的核心设计思想是通过增加冗余信息，使得原始信息的编码之间有足够大的区别。

9.3.1 编码距离

蛋蛋表白时的信息为“我喜欢你”四个字，为了防止女神听不到，他添加了冗余信息。经过蛋蛋添加冗余后变为了“我我我喜喜喜欢欢欢你你你”，其实女神收到的信号为（我我饿Txx欢花欢xx里），其中x表示为邻座大妈的霸气笑声，女神是如何正确地捕捉到蛋蛋意图的呢？显然女神在这方面很有经验，识破了蛋蛋重复三遍的伎俩，电光火石间，在她脑海里飞速搜索比对推理，得出一个通顺而有意义的结论。换句话说，在女神的词典中，有意义的语句全都列出来，发现跟蛋蛋发出声音最相似的就是：“我我我喜喜喜欢欢欢你你你”。

女神的词典可以看成所有可能编码的集合，如何衡量这个编码集合中容易混淆的程度呢？这个参数就是编码距离。什么是距离呢？这里的距离指的是汉明距离，即两个信号之间有多少bit不同。比如信号（0, 1, 1）与（0, 0, 0）的距离为2，（1, 1, 1）与（0, 0, 0）的距离为3。

蛋蛋有4个信息，为00, 01, 10, 11。现在如何插入冗余呢？

首先想到的是重复法：

·00变为00000000；

·01变为01010101；

·10变为10101010；

·11变为11111111。

现在接收到的信号为00010000，我们发现跟这个信号最相似的是00000000，距离为1。

一个编码集合里，大家不一定是均匀分布的，有些编码之间距离比较近，有些比较远，编码距离指的是最近的两个编码之间的距离。

解码的时候，一个最暴力的方法就是一一比较接收到的信号和所有有效编码之间的编码距离，选择编码距离最小的。所以编码距离的重要作用是可以指示编码纠错的bit个数。蛋蛋和阿呆住在不同的地方，相距为 d 。蛋蛋养了一群羊，阿呆也养了一群羊。羊会乱跑，显然只要羊跑的距离小于 $d/2$ ，就可以判断羊属于蛋蛋还是阿呆。所以对纠错码而言，编码距离为 d ，只要bit翻转个数小于 $d/2$ ，我们就可以根据离谁近就归谁的原则去纠错（赶羊回家）。

9.3.2 线性纠错码的基石——奇偶校验 (Parity-Check)

收钱的阿姨狐疑地拿起蛋蛋递过来的100块钱，迎着灯光仔细打量过后，又取出了紫外线灯从头到尾照了一下，终于把钱放进钱盒子里，找了蛋蛋99块5。阿姨担心收到假币，她检查钞票可不敢马虎。

阿姨检查钞票的行为叫信号校验，信号校验的基本模型是：对信号进行某种特定的处理后，得到期望的结果是为校验通过，否则校验失败。

这里信号用 y 表示，特定的处理用 H 表示。 H 表示对信号 y 进行了处理。处理结果用 CR 表示。

$$CR = H(y) = \begin{cases} 0, & \text{校验通过} \\ 1, & \text{校验失败} \end{cases}$$

在二进制的世界里，最基础的校验方法是奇偶校验，即Parity-Check。

对于 n bit二进制信号：

$$CR = H(y) = \begin{cases} 0, & 1 \text{ 的个数为偶数} \\ 1, & 1 \text{ 的个数为奇数} \end{cases}$$

例如长度为16的二进制数据：1000100111011011，其中1的个数为9，故 $CR=1$ 。

判断信号里的1的个数为奇还是偶，有非常简单的方法。在二进制里，有一种异或（即xor）运算，符号为 \oplus ，运算方式是先进行加法运算，然后用运算结果对2取余数（ $\text{mod}(2)$ ），或者更简单地记为“相加不进位”（见图9-5）。

表达式	结果
$0 \oplus 0$	0
$0 \oplus 1$	1
$1 \oplus 0$	1
$1 \oplus 1$	0

图9-5 异或运算表达式

可以验证只要把二进制的每一个bit依次进行xor运算，奇数个bit 1的结果为1，偶数个bit 1的结果为0，与bit 0的个数无关。

所以，用 y_i 表示第i bit的值（0或1），有

$$CR = H(y) = y_1 \oplus y_2 \oplus y_3 \dots \oplus y_n$$

利用奇偶校验可以构造最简单的校验码——单bit校验码SPC（即single bit parity check code）。

把长度为n的二进制信息增加1bit y_{n+1} 变成 y' ，使得：

$$CR = H(y') = y_1 \oplus y_2 \oplus y_3 \dots \oplus y_n \oplus y_{n+1} = 0 \quad (a)$$

现在 y' 构成了 y 的单bit校验码。（a）又叫作奇偶校验方程。

显然， y' 中任意一个bit如果发生bit反转，无论从0到1，还是1到0，校验方程 $CR=1$ 。

SPC可以探知任意单bit的反转。对于偶数个bit反转SPC无法探知。而且校验方程无法知道bit反转的位置，所以无法纠错。

一个自然的想法是，增加SPC的个数，增加冗余的校验信息。同一个bit被好几个校验方程保护，当它出现错误时就不会被漏掉。

后面的文章中，用+代替 \oplus 。

9.3.3 校验矩阵H和生成矩阵G

蛋蛋的丈母娘在女儿结婚前对未来女婿有一个要求列表，前五条是：①要求有博士学位，②脾气要好，③人要长得帅，④会做家务，⑤收入上交。

这样，蛋蛋的丈母娘通过提出要求，就轻而易举实现了对地球上所有男性同胞的一个划分。每一条要求都是一个校验方程。什么样的校验方程组，决定了这个男性同胞群到底由哪些人组成。

多个校验方程可以表示为校验矩阵H。有了H就可以确定所有正确的码字。

对于所有 \mathbf{x} ($x_0, x_1, x_2, x_3, x_4, x_5 \dots$)，只要满足 $\mathbf{H}\mathbf{x}^T = 0$ ， \mathbf{x} 就是正确的码字。如果不满足，则 \mathbf{x} 不属于正确的码字，认为在传输的过程中 \mathbf{x} 出现了错误。

举例：长度为4的信号， \mathbf{x} (x_0, x_1, x_2, x_3)，有两个校验方程：

$$x_0 + x_2 = 0$$

$$x_1 + x_2 + x_3 = 0$$

现在用+代替 \oplus ：

$$x^T = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

$$Hx^T = \begin{pmatrix} x_0 + x_2 \\ x_1 + x_2 + x_3 \end{pmatrix}$$

可见， H 矩阵里每一行可以表示一个校验方程。行里的1的位置*i*表示信号中第*i* bit参与校验方程。

所有满足奇偶校验方程的 x 组成了一个编码集合。一般来说，编码长度为*n* bit，有*r*个线性独立的校验方程，则可以提供*k*= (*n-r*) 个有效信息bit和*r*个校验bit。

对于线性分组编码而言，原始信号u经过一定的线性变换可以生成纠错码c，完成冗余的添加。线性变换可以写成矩阵的形式，这个矩阵就是生成矩阵G，表示为c=uG。

其中，c为*n* bit信号，u为*k* bit信号，G为*k*×*n*大小的矩阵。由H矩阵可以推导出生成矩阵G。

9.4 LDPC码原理简介

在纠错码的江湖里，LDPC以其强大的纠错能力，得到了广大工程师的青睐，是目前最主流的纠错码。本节将带领大家一睹LDPC的风采。

9.4.1 LDPC是什么

LDPC全称是Low Density Parity-Check Code，即低密度奇偶校验码。LDPC的特征是低密度，也就是说校验矩阵H里面的1的分布比较稀疏。

比如：

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

LDPC又分为正则LDPC（regular LDPC）和非正则LDPC（irregular LDPC）编码。

正则LDPC保证：校验矩阵每行有固定J个1，每列有固定K个1。

非正则LDPC没有上述限制。

举例，长度为12的LDPC编码C，满足下列校验方程：

$$C_3 \oplus C_6 \oplus C_7 \oplus C_8 = 0$$

$$C_1 \oplus C_2 \oplus C_5 \oplus C_{12} = 0$$

$$C_4 \oplus C_9 \oplus C_{10} \oplus C_{11} = 0$$

$$C_2 \oplus C_6 \oplus C_7 \oplus C_{10} = 0$$

$$C_1 \oplus C_3 \oplus C_8 \oplus C_{11} = 0$$

$$C_4 \oplus C_5 \oplus C_9 \oplus C_{12} = 0$$

$$C_1 \oplus C_4 \oplus C_5 \oplus C_7 = 0$$

$$C_6 \oplus C_8 \oplus C_{11} \oplus C_{12} = 0$$

$$C_2 \oplus C_3 \oplus C_9 \oplus C_{10} = 0.$$

用校验矩阵表示为:

$$\begin{pmatrix} C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} & C_{12} \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} C_3 \oplus C_6 \oplus C_7 \oplus C_8 = 0 \\ C_1 \oplus C_2 \oplus C_5 \oplus C_{12} = 0 \\ C_4 \oplus C_9 \oplus C_{10} \oplus C_{11} = 0 \\ C_2 \oplus C_6 \oplus C_7 \oplus C_{10} = 0 \\ C_1 \oplus C_3 \oplus C_8 \oplus C_{11} = 0 \\ C_4 \oplus C_5 \oplus C_9 \oplus C_{12} = 0 \\ C_1 \oplus C_4 \oplus C_5 \oplus C_7 = 0 \\ C_6 \oplus C_8 \oplus C_{11} \oplus C_{12} = 0 \\ C_2 \oplus C_3 \oplus C_9 \oplus C_{10} = 0 \end{matrix}$$

我们看到H矩阵每行有4个1，每列有3个1，所以C为正则LDPC。

9.4.2 Tanner图

讲到LDPC，少不了Tanner图，H矩阵可以直观地表示为Tanner图。Tanner图由节点和连线组成。

节点有两种：一种叫b节点（bit node），一种叫c节点（check node）。

假设信号编码长度为n，其中每一个bit用一个b节点表示。校验方程个数为r，每一个校验方程用一个c节点表示。

现在连线，如果某个b节点 b_i 参与了某个c节点 c_j 的校验方程，则把b节点 b_i 和c节点 c_j 连起来。

注意b节点用圆形表示，c节点用方块表示。每个b节点和3个c节点相连，每个c节点和4个b节点相连，如图9-6所示这是一个典型的正则LDPC。

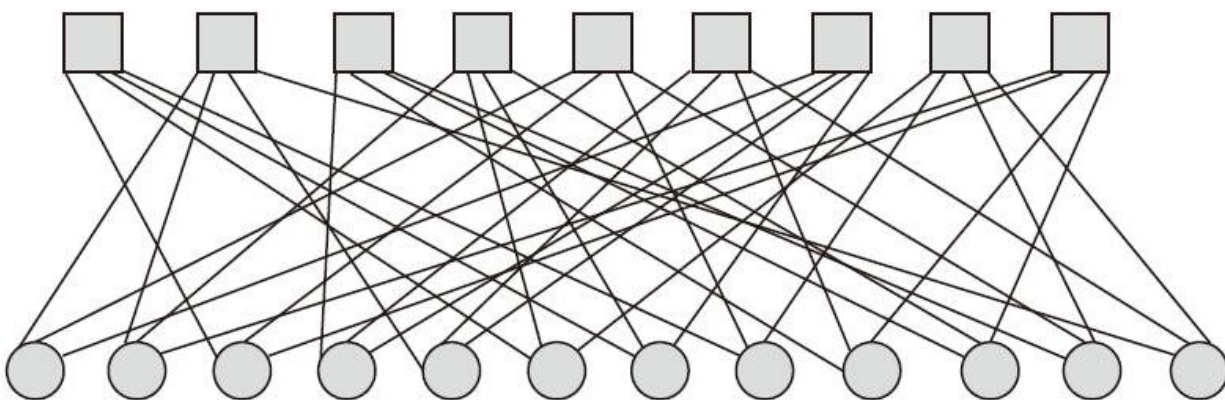


图9-6 Tanner图

Tanner图把编码和图论神奇地结合在了一起。有了Tanner图，LDPC的解码方法就比较好阐述了。

9.5 LDPC解码

LDPC的解码方法有硬判决解码（hard decision decode）和软判决解码（soft decision decode）两种。

本节将介绍一种经典的硬判决算法——Bit-flipping算法和一种软判决算法——和积信息传播算法。

9.5.1 Bit-flipping算法

Bit-flipping算法的核心思想是：如果信号中有一个bit参与的大量校验方程都校验失败，那么这个bit有错误的概率很大。

好的校验方程可以达到上述效果。校验矩阵的稀疏性把信号的每个bit尽量随机地分散到多个校验方程中去。Bit-flipping算法运用消息传递方法，通过不断迭代达到最终的纠错效果。

Bit-flipping解码算法如下：

给定一个 n bit信号 y (y_1, y_2, \dots, y_n)，校验矩阵 H 。画出 H 矩阵对应的Tanner图。 n bit信号对应 n 个b节点， r 个c节点。

1) 每个b节点向自己连接的c节点发送自己是0还是1。初始是第 i 个bit发送初始值 y_i 。

2) 每个c节点收到很多b节点的信息，每个c节点代表一个校验方程。

·如果方程满足，c节点将每个b节点的消息原封不动地发送回去。

·如果校验失败，c节点将每个b节点发来的消息取反后，发送回去。

3) 每个b节点跟好多c节点相连，b节点收到所有来自c节点的消息后，采用投票法来更新这一轮输出的消息。参加投票的包含每个bit的初始值。投票的原则是少数服从多数。

4) b节点更新好后，停止条件：所有的校验方程满足或者迭代次数超过上限。如果停止条件不满足，则需要转到步骤1继续迭代。

下面举个例子：

输入信号 $y=[1\ 0\ 1\ 0\ 1\ 1]$ ，经过步骤1后，如图9-7所示，实线箭头表示传递的信息为1，虚线箭头表示传递的信息为0。

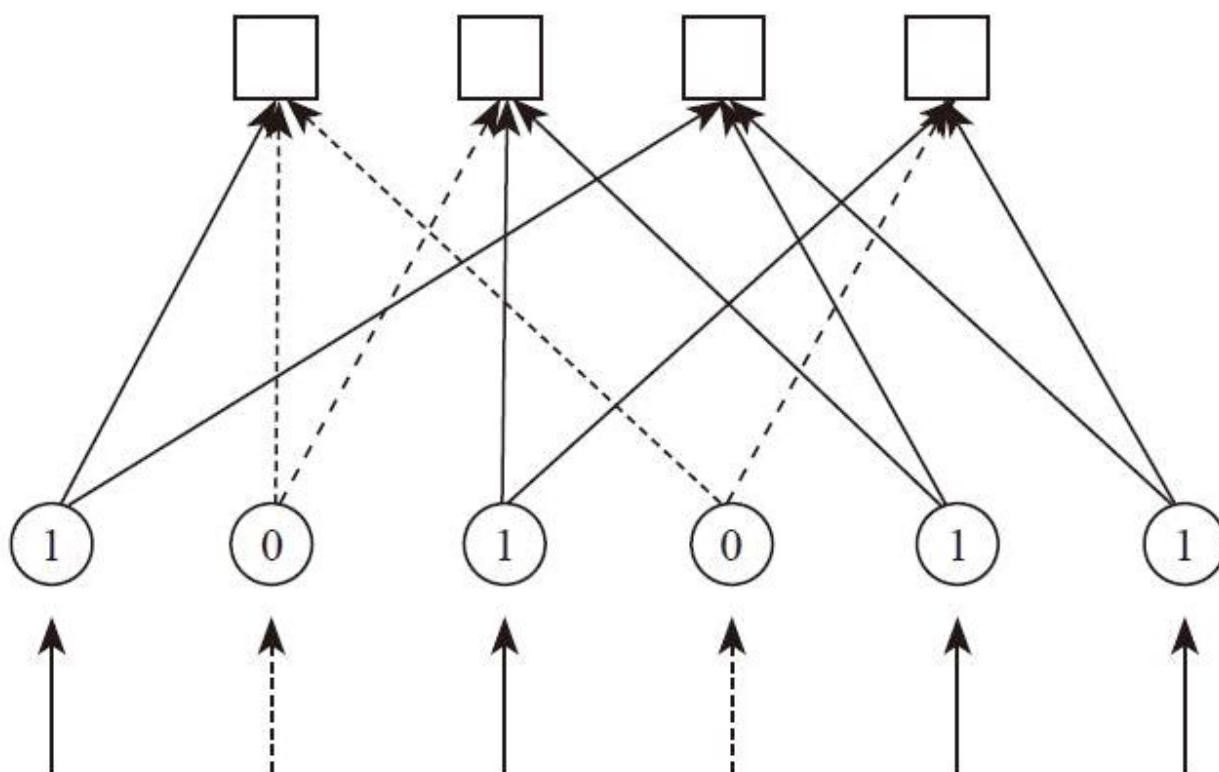


图9-7 步骤1

经过步骤2，c节点给各个b节点发回消息。满足校验方程的c节点原封不动返回消息，不满足则取反返回，如图9-8所示。

步骤3，投票法表决并重新更新b节点的值，如图9-9所示。

步骤4，重新检查节点，发现校验方程满足，结束，如图9-10所示。

Bit-flipping算法有很多细节值得讨论。

其中一个问题是，b节点更新时，一次更改一个还是一次更改多个，或者两者结合。因为校验矩阵的结构，如果同时改变很多b节点的话，可能无法收敛。这时可以将梯度下降法应用到**Bit-flipping**算法中。通过构造目标函数，目标函数包括校验方程最小误差，以及与原信号最大相似，来更新b节点。最终的结论是，每次单个bit翻转的收敛性好，但是比较慢，如图9-11a所示，翻转多个的话会导致收敛性震荡，但是速度快。一个中间方案是，先进行多个bit的翻转，等校验方程失败的个数小到一定程度后，再进行单个bit翻转。

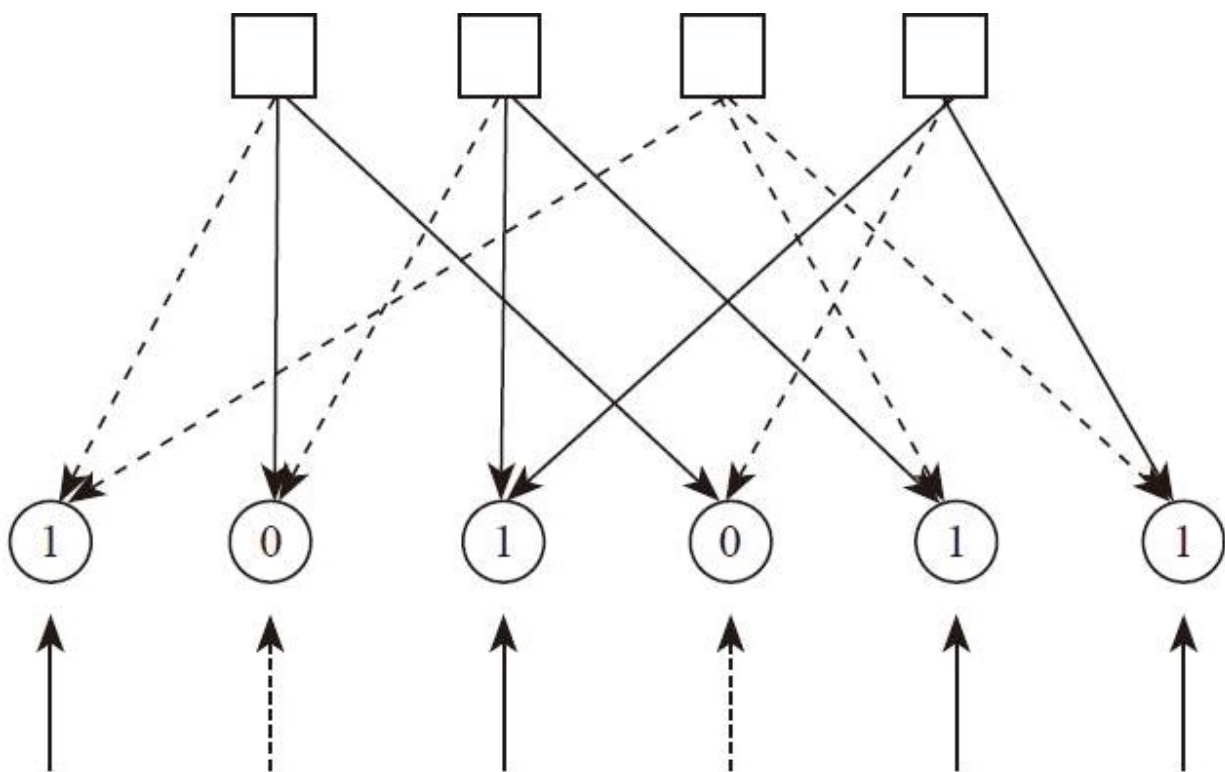


图9-8 步骤2

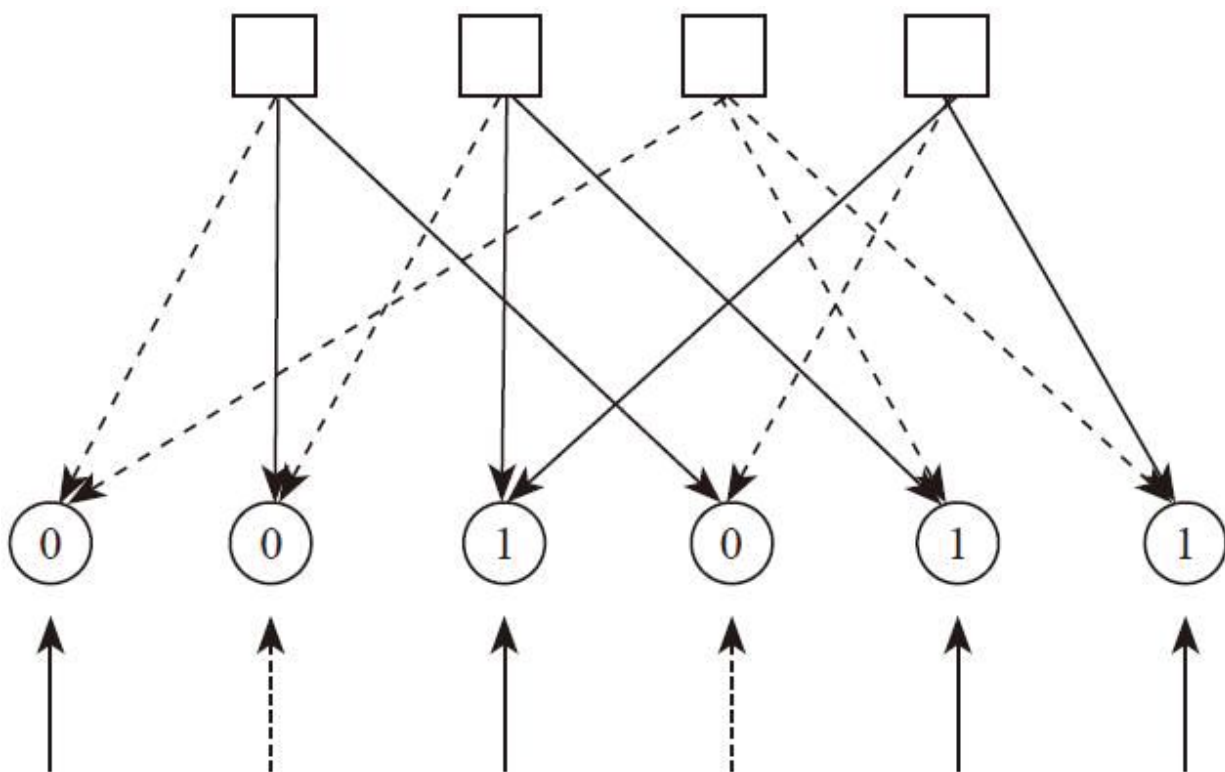


图9-9 步骤3

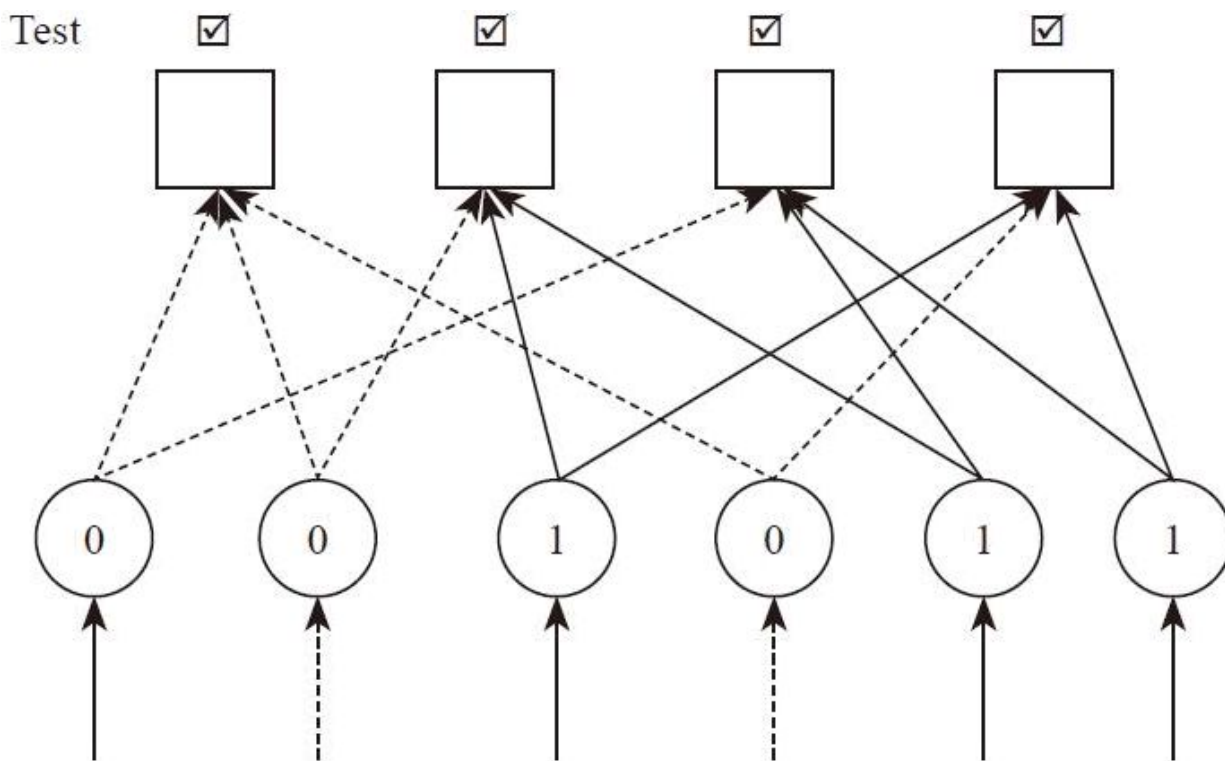


图9-10 步骤4

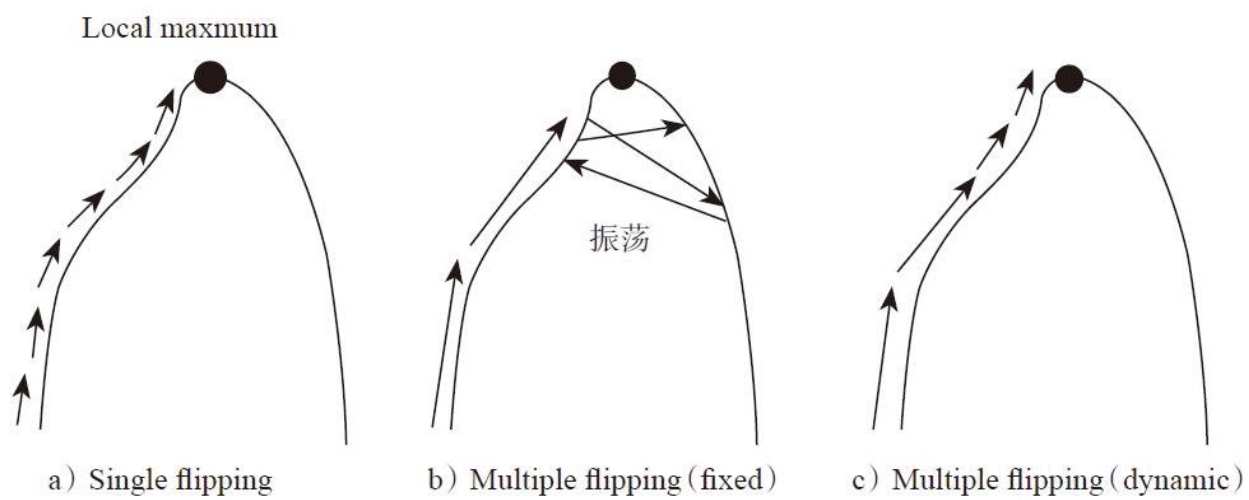


图9-11 几种Bit-flipping算法收敛示意图

9.5.2 和积信息传播算法

这一节我们来介绍和积信息传播算法（**sum-product message passing**，简称和积算法），它是在贝叶斯网络、马尔可夫随机场等概率图模型中用于推断的一种信息传递算法。目前广泛应用于人工智能和信息处理领域，而它的一个非常经典的应用就是LDPC码。

该算法的基础是概率论，这里假定读者的概率论知识没有全部还给老师。

什么是条件概率？什么是联合概率？什么是边缘概率？

条件概率 $P(A|B)$ 表示在事件B的条件下，发生事件A的概率。

$P(B|A) = P(A, B) / P(A)$ 。其中 $P(A)$ 、 $P(B)$ 分别表示随机事件A、B发生的概率。

$P(A, B)$ 表示事件A和事件B共同发生的概率，也叫联合概率。

而且我还知道，贝叶斯公式： $P(B|A) = P(A|B) \cdot P(B) / P(A)$

边缘概率则是指从多元随机变量中的概率分布得出的只包含部分变量的概率分布，比如 $P(A)$ 。

根据联合概率函数如何计算其他类型的概率？举个例子，联合概率 $P(A, B, C, D) = f(A, B, C, D)$ ，则边缘概率 $P(A)$ 的概率要把B, C, D所有取值都遍历一遍。

$$P(A) = \sum_B \sum_C \sum_D f(A, B, C, D)$$

$$P(A|B=1) = \sum_C \sum_D f(A, B=1, C, D)$$

有时候随机变量内部之间有约束关系，这种情况下，可以化简很多运算。

什么是贝叶斯网络（**Bayesian networks**）？贝叶斯网络是一种推理性图模型。贝叶斯网络可以帮助你更好地分析问题。比如如下网络，

w 、 x 、 y 、 z 分别表示4个随机事件， w 表示一个人是否吸烟， x 表示其职业和煤矿是否相关， y 表示其是否患有咽炎， z 表示其是否得肺部肿瘤，如图9-12所示。

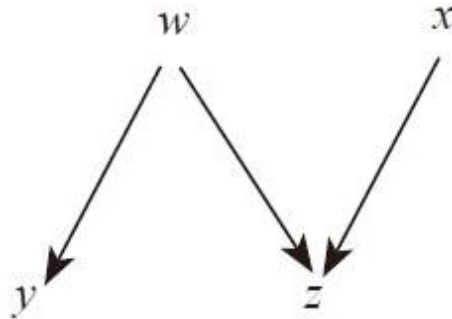


图9-12 一个贝叶斯网络例子

贝叶斯网络有以下关系：

$$P(w, x, y, z) = P(w) P(x) P(y|w) P(z|w, x)$$

我们只要知道了 $P(w)$ 、 $P(x)$ 和 $P(y|w)$ 、 $P(z|w, x)$ ，那么网络模型就构建出来了。 $P(w)$ 表示一个人抽烟的概率， $P(x)$ 表示职业和煤矿相关的概率，这两个可以用社会平均统计数据。 $P(y|w)$ 表示吸烟与否的条件下得咽炎的概率。 $P(y|w=1)$ 表示吸烟者得咽炎的概率。 $P(y|w=0)$ 表示不是吸烟者得咽炎的概率。 $P(z|w, x)$ 表示考虑是否吸烟和是否在煤矿工作的情况下肺部得肿瘤的概率。

这个网络建立起来后，当 w 、 x 、 y 、 z 发生任意一件或者几件事情的时候，我们可以求其他事件的后验概率。比如，当 $y=1$ 时，即得咽炎的情况下，我们可以通过网络算出 $P(z|y=1)$ 即得咽炎的情况下得肺部肿瘤的概率。当 $z=1$ 时，即得肺部肿瘤的情况下，我们可以反推算出 $P(w|z=1)$ 即得肿瘤的情况下吸烟的概率。

什么是因子图？因子图是无向的概率分布二部图。所谓因子，由于事件之间有内在的约束关系所表现出来的一种逻辑形式，比如一种联合概率可以表示为：

$$P(A, B, C, D, E, F, G) \propto f_1(A, B, C, D, E, F, G) = f_1(A, B, C) f_2(B, D, E) f_3(C, F) f_4(C, G)$$

在这种情况下，联合概率可以分成因子乘积的形式。上式 f_i 中叫作约束方程。 $f_i (S_i)$ 表示第 i 个因子，用 S_i 来表示其约束的随机变量组合，如 $S_1=\{A, B, C\}$ 。

例如： $P(A) \propto \sum_{B, C, D, E, F, G} \prod_i f_i (S_i)$

用因子图来表示（见图9-13）：

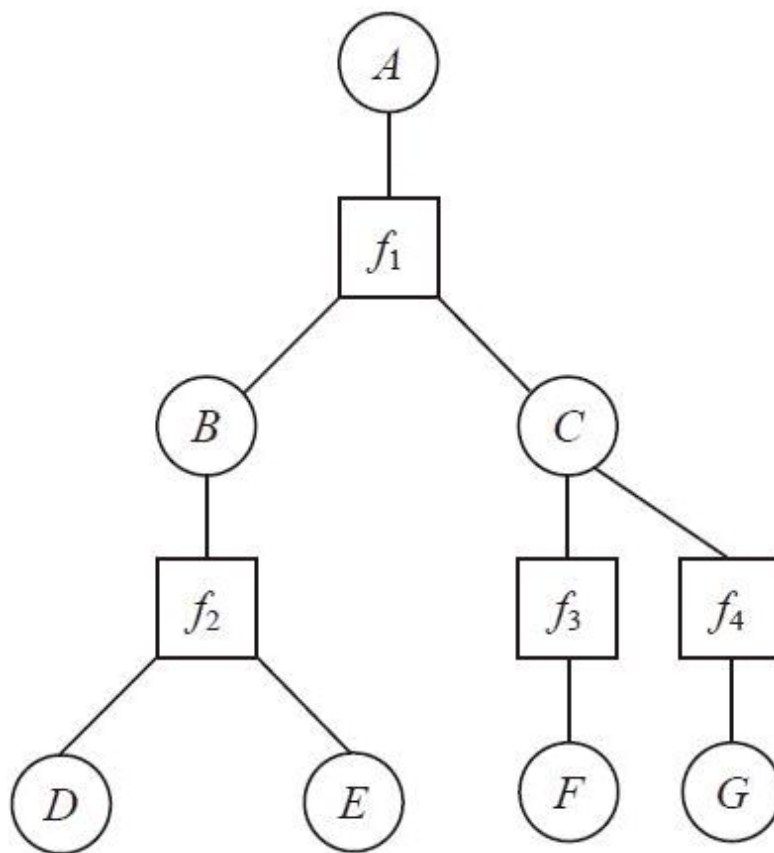


图9-13 一个因子图的例子

这样我们再求解边缘概率就比较简单了，为什么呢？根据小学学过的数学知识——乘法分配律：

$$xy_1 + xy_2 = x (y_1 + y_2)$$

左式用了两次乘法，一次加法；右式用了一次乘法，一次加法。

所以： $\sum_i xy_i = x \sum_i y_i$

乘-加变换为加-乘后，计算复杂度降低。当我们计算边缘概率或者其他形式的概率时，这个特性非常重要。

现在求P (A)：

$$\begin{aligned}
 P(A) &\propto \sum_{B,C,D,E,F,G} \prod_i f_i(S_i) \\
 &= \sum_{B,C,D,E,F,G} f_1(A,B,C) f_2(B,C,D) f_3(C,F) f_4(C,G) \\
 &= \sum_{B,C,D,E} f_1(A,B,C) f_2(B,D,E) \sum_F f_3(C,F) \sum_G f_4(C,G) \\
 &= \sum_{B,C,D,E} f_1(A,B,C) f_2(B,D,E) m_{c3}(C) m_{c4}(C) \\
 &= \sum_{B,C,D,E} f_1(A,B,C) f_2(B,D,E) m_c(C) \\
 &= \sum_{B,C} f_1(A,B,C) \sum_{D,E} f_2(B,D,E) m_c(C) \\
 &= \sum_{B,C} f_1(A,B,C) m_b(B) m_c(C) \\
 &= f(A)
 \end{aligned}$$

其中： $m_b(B) = \sum_{D,E} f_2(B,D,E)$ ， $m_{c3}(C) = \sum_F f_3(C,F)$ ， $m_{c4}(C) = \sum_G f_4(C,G)$ ，

$$m_c(C) = m_{c3}(C) m_{c4}(C)$$

有了上边的公式，最终得到： $P(A) \propto f(A)$ ， $f(A)$ 就是上面最终计算出的只跟A有关系的函数。

故可以设 $P(A) = K f(A)$ ，K为归一化因子。结合归一化方程：

$$P(A=0) + P(A=1) = 1$$

可以求得 $P(A)$ 。

上面的推导过程看上去很复杂，其实就是乘法结合律的应用而已，而且可以明显看到求边缘概率的过程就是一个乘积然后相加的过程，所以叫和积（sum-product）。而且 m_b 和 m_c 只和自己的约束方程有关。在图9-14中可以看到，这种优化的算法看上去像信息在传播。推而广之，如果图很复杂，我们也可以这样计算。从要求的节点A看，总可以看到因子图是一棵树，而A是根节点，A的边缘分布可以看作消息层层传递的过程。

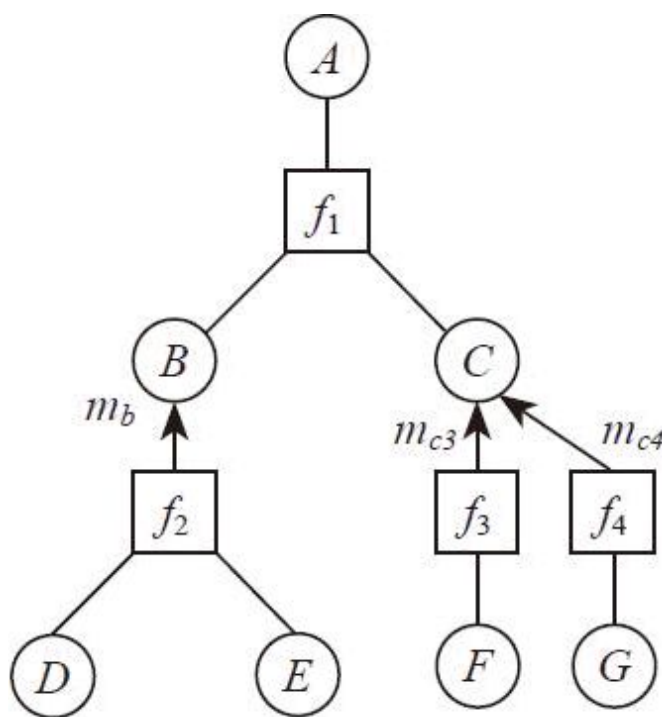


图9-14 m_b 和 m_c 在图上的表示

了解了可能涉及的数学知识，那么和积算法怎么应用呢？

此处为了讨论方便，用 X 表示真实信息，用 Y 表示随机观测信号，可以是电压值，也可能是探测阈值（因为软判决算法可以利用比硬判决算法更多的信道信息，如图9-15所示）。

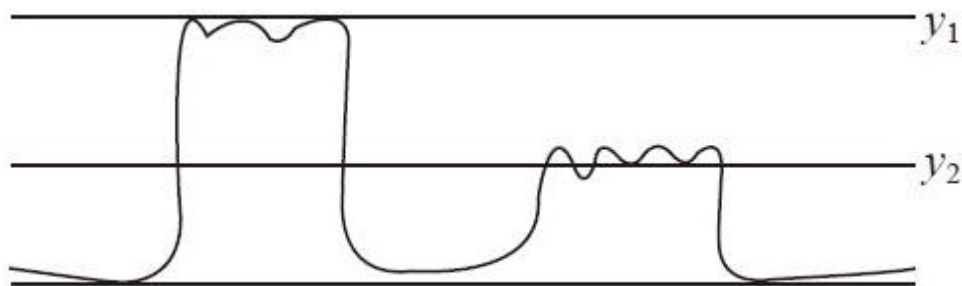


图9-15 两个 $X=1$ 的信号 $P(X=1|Y=y_1)=0.9$ (左) , $P(X=1|Y=y_2)=0.6$ (右)

我们建一个模型，没错就是Tanner图，Tanner图也是一种因子图。

如图9-16所示，每个涂色方块表示一个c节点，代表一个校验方程，而校验方程是一种非常简单的约束方程。举个例子：

$$f(A,B,C)=\begin{cases} 1, & \text{当 } A+B+C=0 \\ 0, & \text{其他情况} \end{cases}$$

每个圆圈表示与b节点对应的 X_i ，而与之前Tanner图不同的是，每个b节点都有唯一的观察约束节点（用空心框图表示）与之绑定。观察约束节点负责提供 $P(X_i|Y_i=y_i)$ ，所以约束方程 $f_Y(X_i)=P(X_i|Y_i=y_i)$ 。

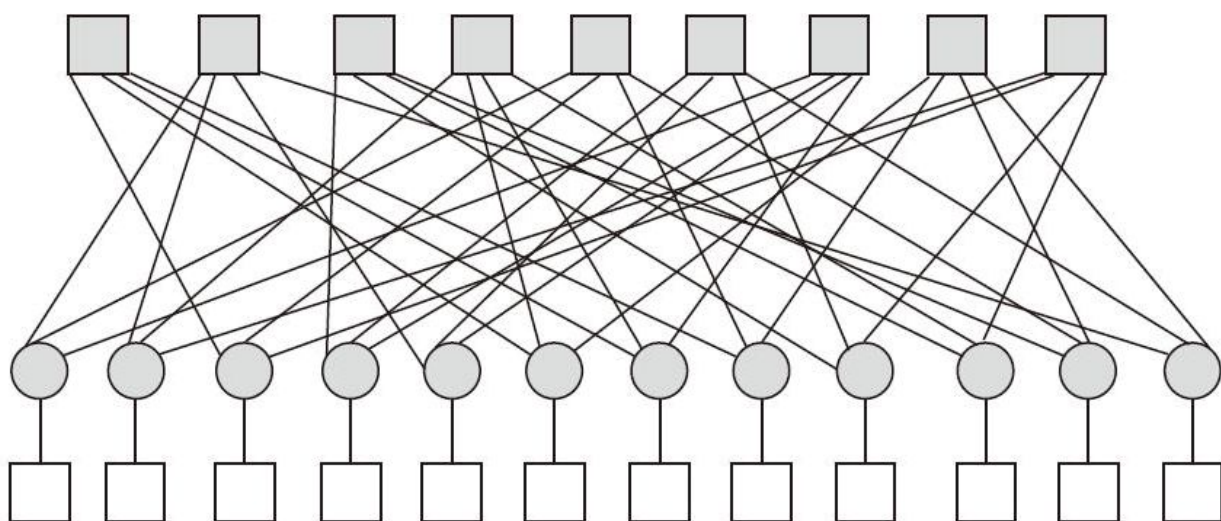


图9-16 Tanner图

我们的目的是，求得每一个边缘概率 $P(X_i)$ 。最终的 $P(X_i) = K f(X_i)$ ， K 为归一化因子。如果 $f(X_i=1) < f(X_i=0)$ ，我们输出 X_i 为0，否则输出1。

下面见证奇迹的时刻到了。

1) 首先假定Tanner图是一棵树（如果不是树，后面有讨论）。

2) 对于任意 X_i ，为了方便称为 A ，我们把它当成根节点，如图9-17所示。

3) 通过消息传播的方法， $P(A)$ 可用如下方法求得：

①从各个叶子节点往根节点传播消息。如图9-18所示，五个 m 都是从信道得来。比如 $m_{f9 \rightarrow A} = f_9(A) = P(A|Y_A=y_A)$

②消息传播到 b 节点（见图9-19中的圆圈）后，由 b 节点继续向根节点方向传播，进入下一个约束方程的范围，穿过约束方程后，原来的消息被汇聚成新的消息，如果有两个约束方程连到同一个 b 节点，则信息相乘后继续传播。图9-19是一个局部示意图。

可以计算 $m_B = \sum_{D, E} f_2(B, D, E) m_D m_E$

③继续传播，直到所有的消息最终传到 A （见图9-20）：

$$P(A) = m_{f9 \rightarrow A} m_{f1 \rightarrow A}$$

这样就求得了 $P(A)$ ，同理其他所有的边缘分布都可以求出来！读者通过观察应该发现，这个消息传播的算法其实可以并行化，只要稍微更改一下算法即可。

下面介绍如何简单地实现并行化。

为了同时求出所有边缘分布，每个 B 节点对消息进行路由。把每个约束方程的方向当成根节点对待，把不是这个方向传来的所有消息相乘之后送出去。收到消息时如图9-21所示。

X 节点发送消息，如图9-22所示。

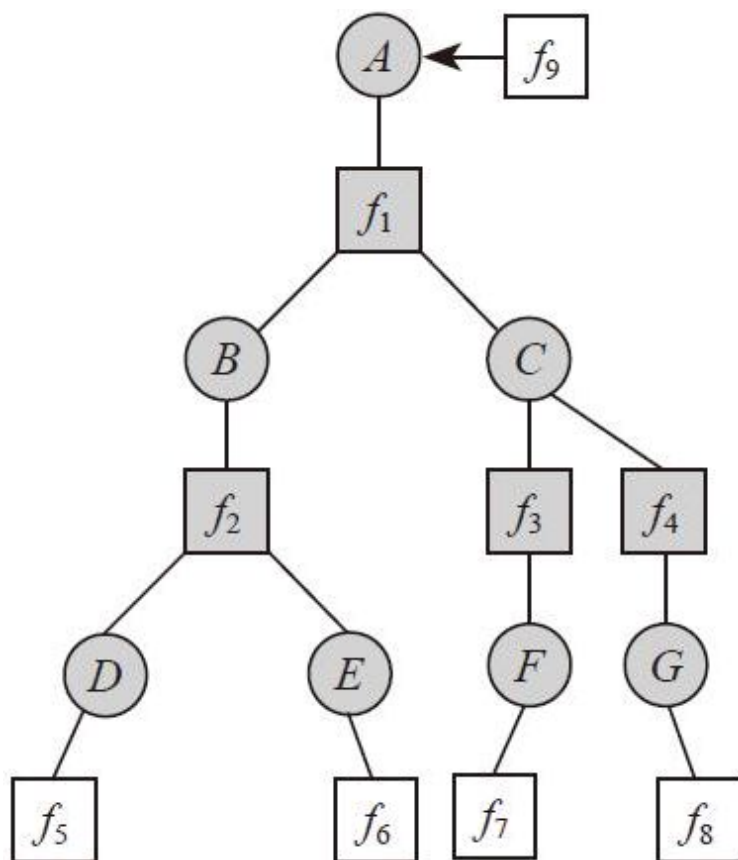


图9-17 一个节点对应一棵树

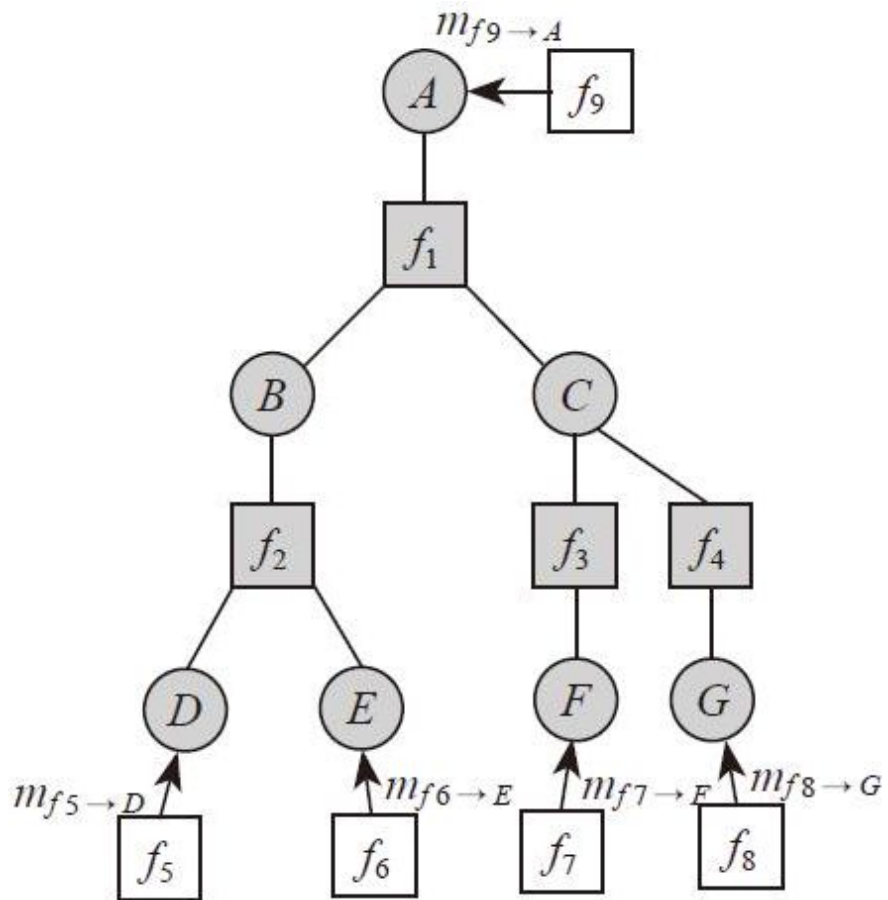


图9-18 消息传播第一步

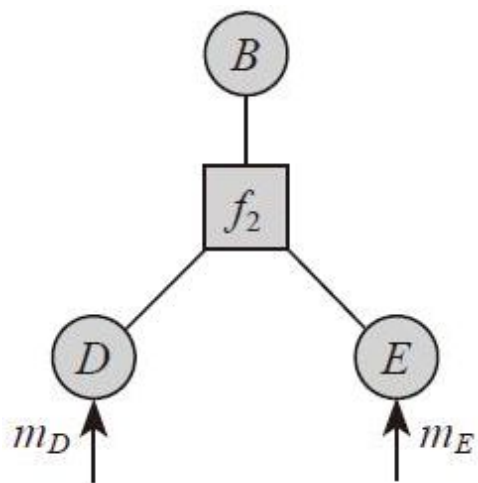


图9-19 一个局部示意图

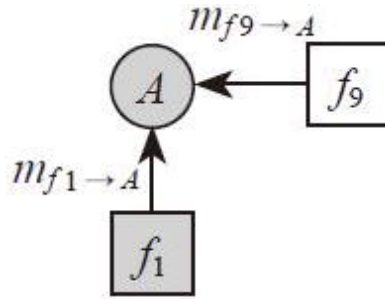


图9-20 最后一步

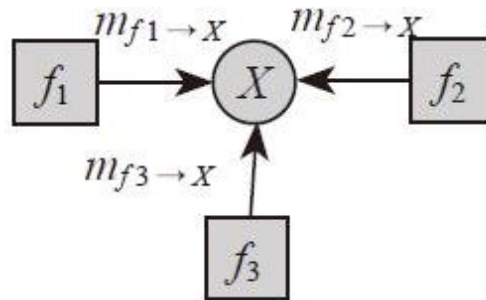


图9-21 收到好多消息的X节点

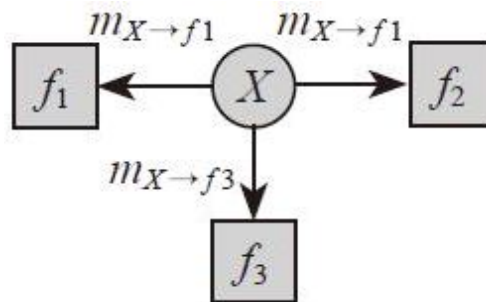


图9-22 X发送给各节点消息

并且满足：

$$m_{X \rightarrow f1} = m_{f2 \rightarrow X} m_{f3 \rightarrow X}$$

$$m_{X \rightarrow f2} = m_{f1 \rightarrow X} m_{f3 \rightarrow X}$$

$$m_{X \rightarrow f3} = m_{f1 \rightarrow X} m_{f2 \rightarrow X}$$

同理每个c节点（约束方程f来表示c节点）也要针对不同的可能路径进行计算。图9-23表示了通往c节点的传播消息。

c节点往各个b节点传送的消息为（见图9-24）：

$$m_{f \rightarrow B} = \sum_{D,E} f(B,D,E) m_{D \rightarrow f} m_{E \rightarrow f}$$

$$m_{f \rightarrow D} = \sum_{B,E} f(B,D,E) m_{B \rightarrow f} m_{E \rightarrow f}$$

$$m_{f \rightarrow E} = \sum_{D,B} f(B,D,E) m_{D \rightarrow f} m_{B \rightarrow f}$$

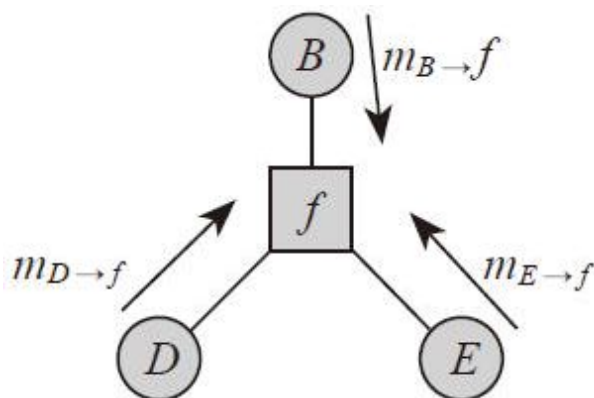


图9-23 通向f约束方程的各个消息

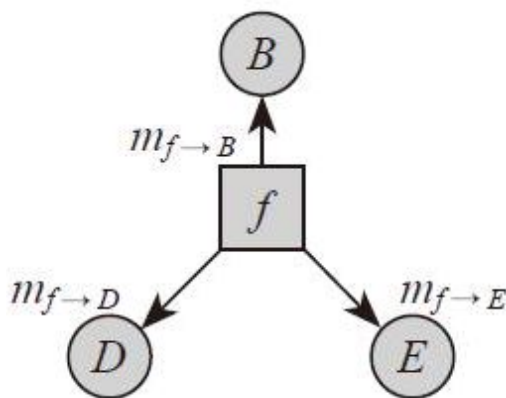


图9-24 c节点往各个b节点传递消息

最终，经过多次迭代（最多为因子图中最大深度树的两倍深度），得到所有节点的边缘概率 P 。算法结束。

值得讨论的是，前边的算法假定Tanner图是无环的，每一个节点都可以拉出一棵树来。在现实中，这个假定是不成立的，但是该算法也有不错的表现，不过环对纠错的成功与否有着很大的影响。

9.6 LDPC编码

LDPC是一种以解码为特点的编码，由于LDPC的性质主要由H矩阵决定，一般先确定H矩阵后，反推回生成矩阵G。

H矩阵构建时候，应当注意：

- 1) 保持稀疏。每行每列里1的个数要固定，或者接近固定。
- 2) 考虑到生成矩阵的计算复杂度。

3) 保持随机性。减少H矩阵里小环的个数。图9-25展示了一个长为4的小环（b节点、c节点和连线组成的环）。

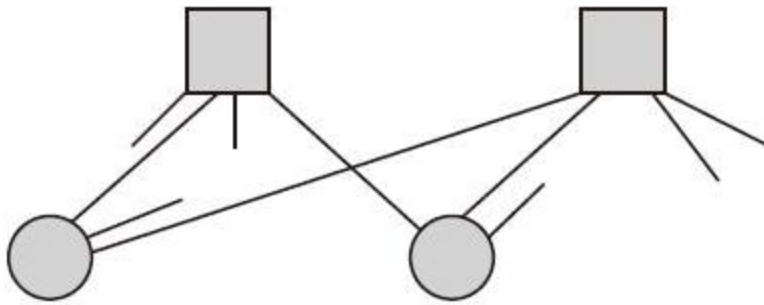


图9-25 Tanner图上的一个小环

显然这两个b节点共同参与了两个相同的校验方程。我们叫它们双胞胎，对bit-flipping而言，假如它们之间有一个错误，我们将无法对错误进行定位。对和积算法而言，环越长，BP算法效果越好。

关于LDPC编码的其他介绍，读者可以参阅最新的学术成果，在此不作展开。

9.7 LDPC在SSD中的应用

本节介绍NAND纠错模型，以及LDPC在SSD中的纠错流程。

9.7.1 NAND会出错

在本书第1章中，我们知道，纠错能力是一个SSD质量的重要指标。最开始的NAND每个存储单元只放一个bit，叫SLC，后来又有了MLC，现在主流的是TLC。在存储密度不断增加的同时，器件尺寸变小，存储单元电气耦合性变得很复杂。比如氧化层变得很薄，比如读取单个bit需要的读电压控制能力更精密等，总的来说，NAND flash更容易出错了，或者说NAND上的噪声增加了。

RBER（Raw Bit Error Rate）是衡量NAND质量的重要参数。给定RBER，可以比较各种纠错算法的有效性，如图9-26所示。

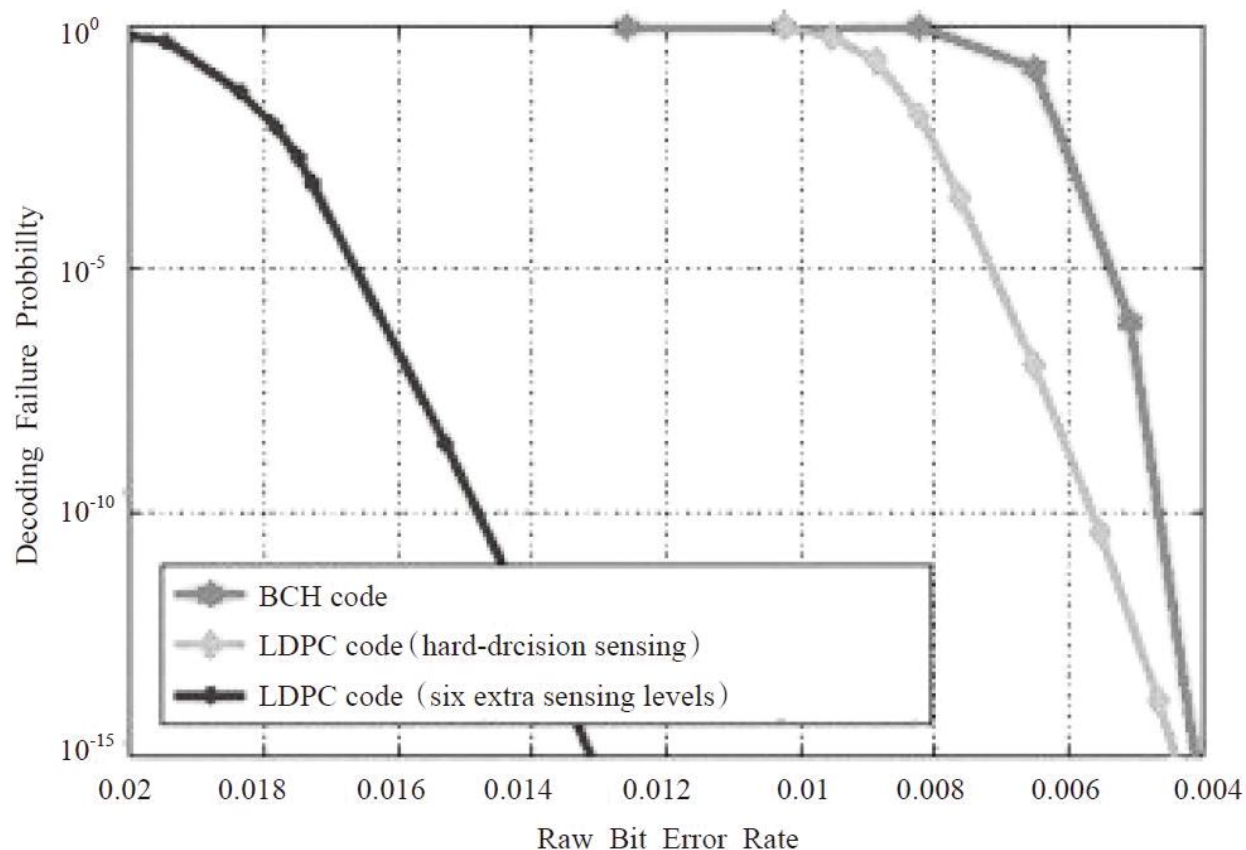


图9-26 曲线从右到左依次是BCH、LDPC硬判决算法、LDPC软判决算法，纵轴表示纠错失败的概率，横轴表示RBER

可以看到，LDPC软判决算法由于有更多的信道信息，相对于BCH和LDPC硬判决算法更有优势。

9.7.2 NAND纠错模型

NAND的基本特性请参阅第3章。我们存储进NAND的信息通过电子储存起来，读的时候通过探测器件储存的电子多少来恢复数据。

信息0和1在NAND上的电压分布图（示意图）如图9-27所示，以SLC为例，该分布可以通过大量的数据探测出来。竖线的横坐标值对应NAND的读取阈值电压。可见，对于1的概率分布在阈值电压右侧的将会被NAND硬判决成0，从而导致bit翻转。

通过调节不同的阈值电压来对NAND进行多次读取，可以获得额外的信息（得到阈值电压在哪个区间），如图9-28所示。利用概率论的知识，可以建立统计模型。

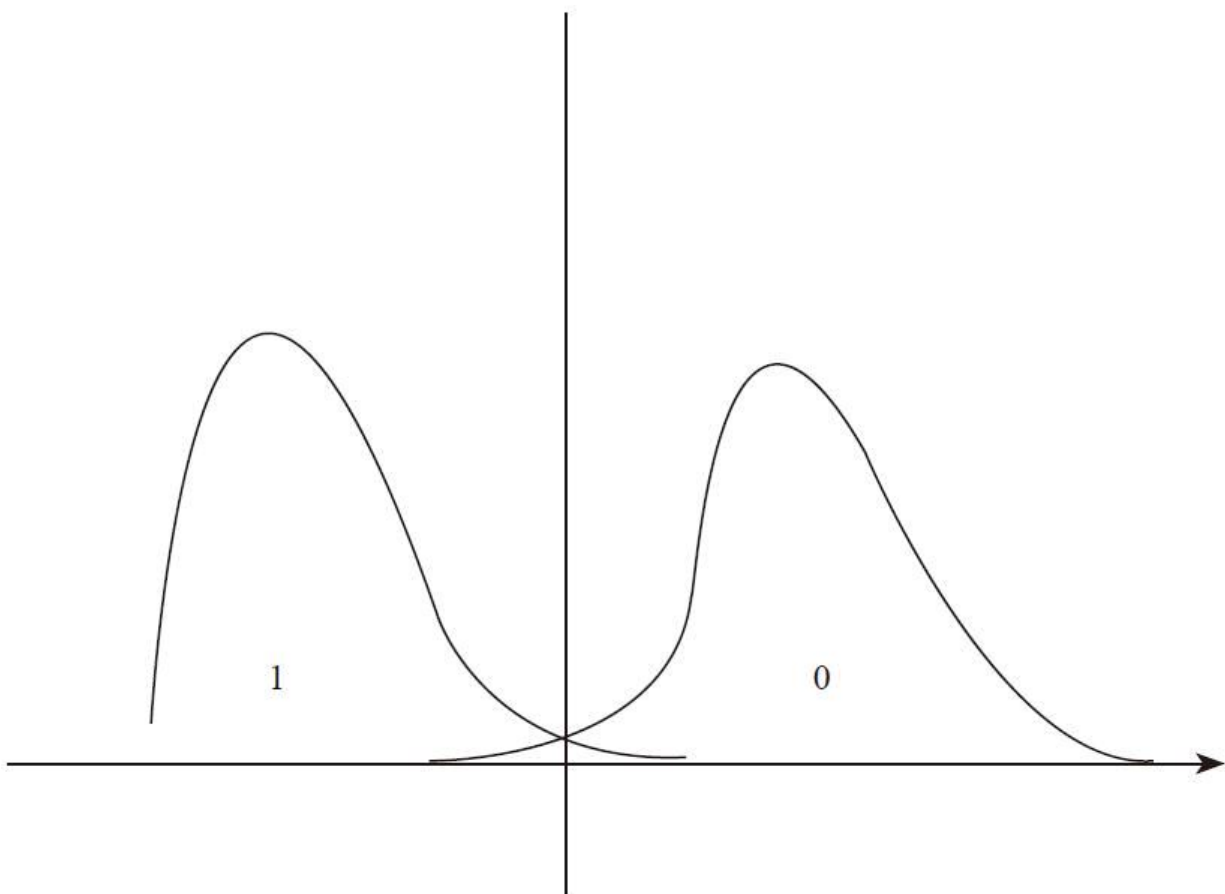


图9-27 SLC两种状态的概率分布示意图，竖线的横坐标值对应阈值电压

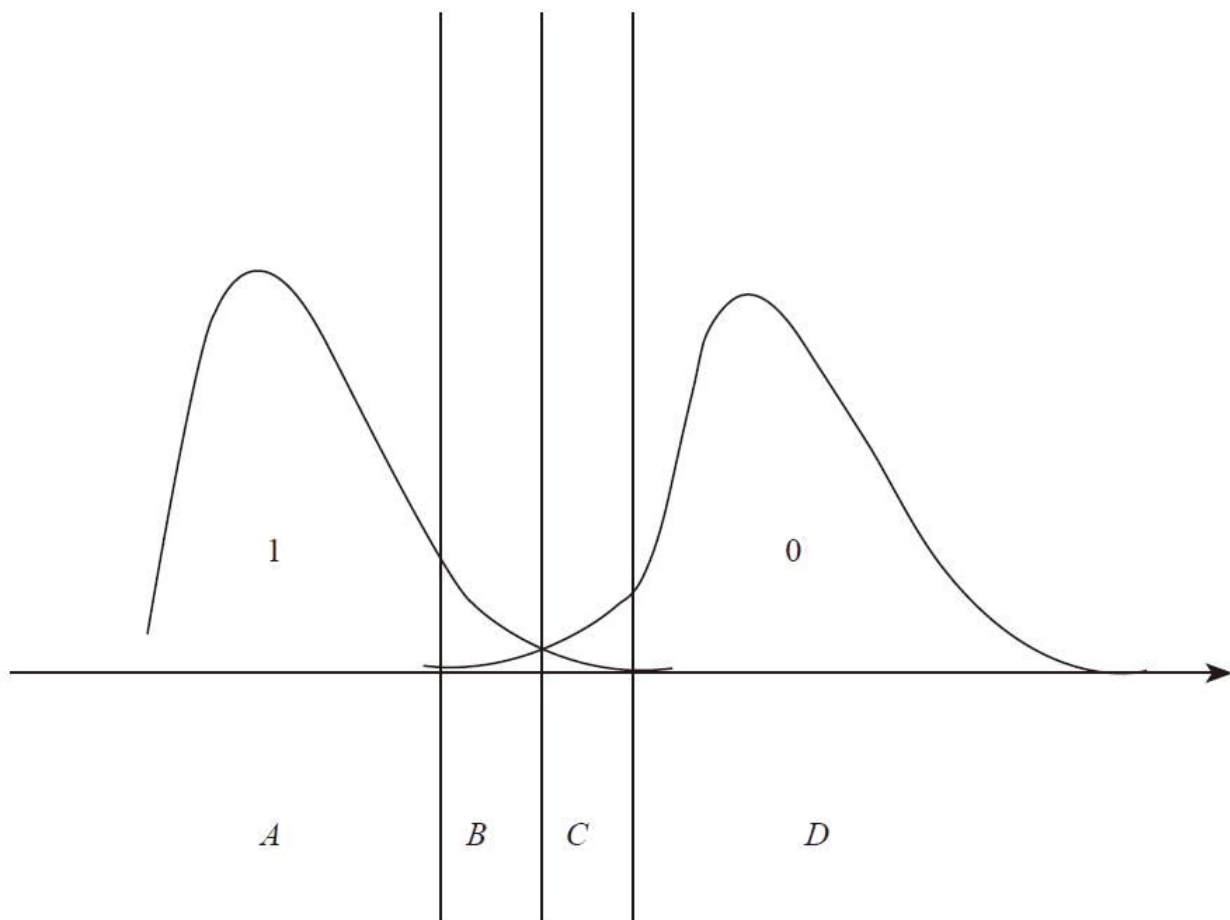


图9-28 多次调整读取电压

假设写入的信息为 X ， X 取值 $\{0, 1\}$ ，其阈值电压为 Y ，调节读取电压阈值后，根据读出值将整个区域分成了4个区间。

图9-28所示的左右两条曲线分别为 $p(Y|X=1)$ 和 $p(Y|X=0)$ 的曲线。根据之前和积算法的介绍，我们感兴趣的是： $P(X|Y=A)$ ， $P(Z|Y=B)$ ， $P(X|Y=C)$ ， $P(X|Y=D)$ 。知道这几个概率后，LDPC软判决算法（如和积算法）就可以工作了。根据前面对条件概率和贝叶斯公式的复习，下面的工作交给读者研究。

9.7.3 LDPC纠错流程

LDPC在SSD中的纠错流程如图9-29所示，值得注意的是，NAND硬判决、数据传输到控制器，以及硬判决解码这几个过程的速度都很快。软判决要读很多次，传输数据很多次，所以会对SSD的性能产生不好的影响。

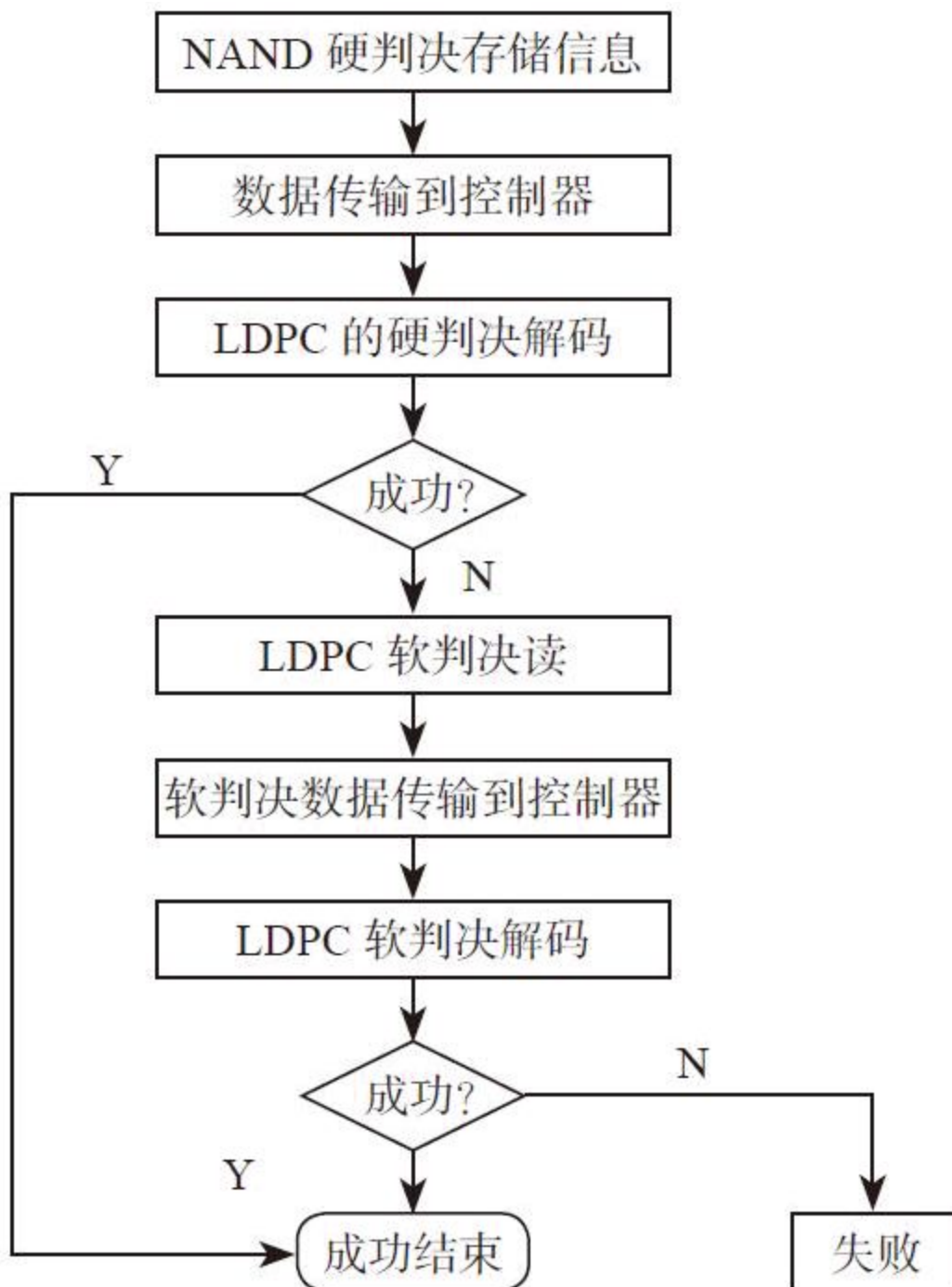


图9-29 LDPC纠错流程

为了提高性能，一种普遍的优化是，把LDPC软判决的分辨率变成动态可调，这样只有在最坏的情况下，才需要最高的分辨率去读。这样在大部分情况下，软判决读和软判决传输数据的时间开销将大幅度减小。